93-00010/

Annual Report
Privacy Commissioner
1991-92

Front Cover: The new "smart cards" look like bank or credit cards but there is an essential difference. Imbedded in the card is a computer chip to process and store data and to identify the owner. The symbols illustrate the range of services and personal information that may soon be stored on one small piece of plastic. They are:

- Telephone calling card
- Bus pass
- Federal benefits
- Banking services
- Retail purchases
- Medical records
- Computer system access
- Residence and workplace access

The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-2410, 1-800-267-0441
Fax (613) 995-1501
TDD (613) 992-9190

© Minister of Supply and Services Canada 1992

Cat. No. IP30-1/1992

ISBN 0-662-59183-6

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

August 12, 1992

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report.

This report covers the period from April 1, 1991 to March 31, 1992.

Yours sincerely,

Bruce Phillips
Privacy Commissioner

The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa

August 12, 1992

Dear Mr. Fraser:

I have the honour to submit to Parliament my annual report.

This report covers the period from April 1, 1991 to March 31, 1992.

Yours sincerely,

Bruce Phillips
Privacy Commissioner

Table of Contents

Mandate 1

The End of the Beginning? 3
Charter privacy protection 8
Privacy in banking and telecommunications 10
The private sector: voluntary action 12
Privacy at work 14
Fine tuning the Act 15
Redefining "personal information" 16
Tightening up disclosures 17
Broadening the injury test 19
"Catch 22" 21

Genetic Testing and Privacy 23

A Year in the Privacy Trenches 27
Telecommunications toys—playing with privacy .. 27
This year's SINs 31
Technology update 34
Data matching 38

Complaints Directorate 41
Some cases 52
Notifying the Commissioner 64
Inquiries—the public talks back 70

Compliance Directorate 75
Trends and problems 75
Contracting out—who's minding the data? 76
Checking employee credit ratings 77
Electronic transmission of personal information .. 78
Who's minding the computer? 79
Upward appraisals 82

Corporate Management Branch 83

Organization Chart 86

Mandate

The *Privacy Act* provides individuals with access to their personal information held by the federal government; it protects individuals' privacy by limiting those who may see the information; and it gives individuals some control over the government's collection and use of the information.

The Act sets out the principles of fair information practices, requiring government to :

- collect only the information needed to operate its programs;
- collect the information directly from the individual concerned, whenever possible;
- tell the individual how it will be used;
- keep the information long enough to ensure an individual access; and
- "take all reasonable steps" to ensure its accuracy and completeness.

Anyone in Canada may complain to the Privacy Commissioner if:

- they are denied any part of the information;
- they are denied their request to correct some of the information on the file — or their right to annotate it;
- the department takes longer than the initial 30 days or maximum 60 days to provide the information;
- the *Info Source* description of the contents of an information bank is deficient in some way;
- the department's listing in the Source does not describe all the uses it makes of personal information;

- an institution is collecting, keeping, using or disposing of personal information in a way which contravenes the *Privacy Act*.

The Privacy Commissioner's investigators examine any file (including those in closed banks) except confidences of the Queen's Privy Council to ensure that government institutions are complying with the Act.

The Act also gives the Privacy Commissioner the power to audit the way government institutions are collecting, using and disposing of personal information.

The End of the Beginning?

It may be tempting fate beyond prudent limits. Nevertheless, with crystal ball and reputation in hand, the author is willing to venture the opinion that the privacy picture is getting a little better.

Not yet the sunlit uplands, to be sure: disaster areas abound, and the rubble of many a previous privacy defeat remains untouched.

But, carrying Churchillian paraphrase to unreasonable limits, one senses that, while we are a long way from the beginning of the end to privacy problems, we may be close to the end of the beginning.

In plain talk, we seem to be getting somewhere.

During the year under review, there were a number of developments on several fronts which suggest the slow-gathering defences of privacy are starting to make themselves felt.

Both inside and outside of government there were hopeful signs of greater recognition of the problems affecting privacy, and a greater willingness to seek remedies. To itemize a few of the more outstanding ones:

• Two more provinces, British Columbia and Saskatchewan, are in the process of creating privacy protection schemes. A third, Alberta, is considering similar action. Inclusion of these three provinces would extend some form of data and privacy protection at provincial levels from Quebec to the Pacific Coast.

• Federal legislative activity in the fields of telecommunications and financial institutions stimulated refreshingly intense focus on their privacy implications, both by the government and in Parliament. Some of the proposed responses, still under study as this report goes to press, could point the way to a breakthrough in the difficult problem of achieving higher levels of privacy protection in the private sector.

• Some of the major players in the commercial field are responding more energetically to the rising level of public concern about the way business handles personal information under its control. Notable in this respect are Canada's direct marketers, who are working on a code of practice which, if adopted, offers promise that those among us who do not wish to receive unsolicited mail and telephonic sales pitches will be provided with a convenient and well-publicized method of avoiding them.

• Though technically not within the year, there was a landmark decision by the Canadian Radio and Telecommunications Commission (CRTC) in the case of "Caller ID". It established a critical precedent by ruling that telephone subscribers who wished to preserve the anonymity of their telephone numbers would not have to pay a special charge. This ruling clearly recognized that in telecommunications, privacy is recognized as a consumer's right, and not merely as a commodity for sale.

Some of these developments will be discussed in more detail later in this report. They do not constitute in any way a comprehensive account of all that has happened in the many areas of life and commerce which had an impact on privacy during the year. They are presented as examples of a hopeful trend. Taken singly or together, they represent something considerably less than dazzling victories, but something considerably more than deadlock.

However, they must be viewed in the context of the larger problem. For example, all the earnest jawboning of privacy advocates so far has had almost no impact on the biggest and most serious privacy issue of all, which is the vast and unregulated traffic in personal information, a business whose monetary value in North America runs into the billions of dollars. A society which casually accepts the existence of dossiers of unknown accuracy in unknown hands on millions of individuals, and with no rights of access and correction, is a society which is recklessly indifferent to preserving that most basic privacy right: the right to some control over what others know about you. Yet this is the situation as it now stands. There is scarcely one among us whose name is not to be found in one, and probably more of those dossiers in the computer banks of the list-makers and the list-marketers.

It is, though, an indifference born largely of ignorance. There is ample and heartening evidence that wherever and whenever the public at large clearly understands the issues and is given an opportunity to influence them, whole armies rise up to mount privacy's barricades, sometimes with dramatic results.

Item: a couple of years ago, a telephone company in the United States asked its subscribers whether they objected to their information in the company files being sold off to other companies. Eight hundred thousand of them so objected, and the idea was dropped. Likewise, a scheme involving one of the major software companies in the United States to market a machine-readable disc containing information on eighty million persons provoked such a storm of controversy that it too was discarded.

Public reaction — often angry — to the explosion of direct marketing illustrates the critical importance of wider knowledge about the issues. While not implying that marketers are devoid of a sense of responsibility, it would be naive not to acknowledge that it is public concern about the means by which these firms acquire their information which is injecting fresh impetus into the industry's efforts to develop an improved privacy code.

Thus greater public understanding of privacy issues in the modern technological context is a desperate necessity. What simpler and more graphic proof is required than our recent experience with cellular telephones?

Many people were surprised to learn from our last annual report that conversations over cellular telephones could be monitored with easily-obtained scanning equipment. The revelation has not lessened the public affection or appetite for these extremely useful inventions, but we're willing to wager it has made many people considerably more sophisticated or guarded in their use of them.

All that was ever missing in the cellular phone revelation was adequate information. Mass media coverage of the observations of this office helped to fill the information gap. But one would never have been created in the first place had industry been required to ensure that its clientele was provided with all the information needed to make informed decisions about the equipment.

The obligation to inform rests upon both the private and public sectors. In the latter area, the only national agency which seeks to maintain an overview of the entire privacy field is the Office of the Privacy Commissioner. It is, therefore, the natural body to play a lead role in the area of public education and communication. Yet it is a fact (which even some parliamentarians are surprised to discover) that the office has no public education mandate. We do what we can, with almost no resources for the purpose, largely through the medium of this report, speeches and conferences as time permits, and of course the attentions of the media.

None of these factors is to be discounted, particularly the last. Yet much more can and should be done. Forgotten, perhaps, is the government's commitment in 1987 to seek a *Privacy Act* amendment to give the office an education mandate. Let us hope this reminder stimulates action.

Over the years, both the incumbent and previous commissioners have discussed the merits or otherwise of extending the reach of the *Privacy Act* to include federally-regulated private businesses such as banks and transportation companies. In the case of the present Commissioner, this option was regarded not as the best thing to be done, but as possibly the only thing that could be done in the face of apparent failure to obtain good privacy protection in the private sector any other way. The urgency of this question is somewhat diluted by the current examination by Parliament of the privacy problems posed by financial and telecommunications legislation. We must await results to determine whether this case-by-case approach is better. But there are distinct advantages in the sectoral approach made possible by the *Bank Act*, in which

privacy rules for specific industries or services could be developed. This approach is now being adopted in the Netherlands. In the case of Canadian banks, both the Canadian Bankers Association and several of its members already have developed privacy codes which with some improvements and modifications, could well form the basis of a set of regulations governing their handling of personal information. The principal element missing from the codes as they now stand is a system of independent oversight and dispute resolution, which the Commissioner feels is essential to ensure compliance and public confidence. In any event, efforts to produce a more alert and informed body politic is a more urgent priority. An informed public is the best defence against abuse. That holds true for privacy as much as it does for democracy as a whole. It is certainly a pre-requisite to any kind of effective defence.

Charter privacy protection

The value of an aware public must also be considered in the context of a nation which still has no constitutional right to privacy. Although there are various laws such as the federal *Privacy Act*, which give citizens some protection in specific areas of information gathering, and although the Supreme Court has defined a privacy right in some cases—principally involving criminal laws—the acceptance of privacy as a basic human right has not yet found its way into our statutes.

This office has sought to correct this oversight by appearing before the Special Joint Committee on a Renewed Canada to urge that a right to privacy be included among its recommendations.

The submission pointed out that a privacy right was included in almost the very first draft proposed by the federal government when it unveiled its *Charter of Rights and Freedoms*, that it is already included in a number of similar documents such as the *Quebec Charter of Rights*, the *Universal Declaration of Human Rights*, the *European Covenant of Human Rights*, and the constitutions of several states of the American union, to name just a few. Moreover, the proposal has already been favorably viewed by the Commons justice committee (in 1987), and had the support of such important Canadian groups as the Canadian Bar Association.

Unfortunately, the proposal did not command majority support of the committee. Although this office of course was not privy to the committee's *in camera* deliberations, we understand some members expressed concern that inclusion of a privacy right might have an adverse impact on other freedoms or rights, such as speech or access to information. It should be pointed out that a privacy right would be subjected to the same test of balancing the private and public well-being that applies to all rights and freedoms now in the *Charter*. The *Charter* expressly directs that these rights are to be exercised in a manner that is reasonable in a free and democratic society, thereby imposing on the courts the duty to seek a balance between competing or conflicting claims.

The fate of this initiative was particularly disappointing in view of the constitutional exhaustion that is likely to ensue when the current round of negotiations concludes, with the dim prospect of re-opening the *Charter* any time soon. All the same, this is unfinished business on the Commissioner's agenda, and the office will continue to press the case.

Privacy in banking and telecommunications

At the federal level, some kind of Great Divide may have been traversed, with the inclusion of language in two important pieces of legislation which makes it possible to accommodate privacy concerns. The first of these is the revised *Bank Act* and associated statutes, which will make possible the cross-ownership of banks, insurance and trust companies. Given the huge holdings of personal information in financial institutions, this office naturally is concerned by the degree to which these data might be shared in future, and to what extent the consent and control by clients and customers will be involved in the process.

The legislation gives the government authority to make regulations covering such personal information exchanges. In April, the Commissioner appeared before the Senate banking committee to urge that Parliament take advantage of this authority and draft such regulations.

The committee evinced considerable degree of interest in this recommendation, and indicated that the Commissioner might be invited to discuss the subject further. At the same time, the Commissioner understands the Department of Finance is also examining the issue.

A telecommunications bill now before Parliament is even more explicit in recognizing protection of privacy as one of its objectives, the first such example known to the Privacy Commissioner apart from the *Privacy Act* itself.

As of this writing, the outcome of these initiatives is still to be determined. However, the Commissioner must record his satisfaction with this evidence of growing understanding of the privacy issue both in the councils of government and in the federal bureaucracy.

In fact, the Commissioner sees in the above developments a possible answer, or the beginnings of an answer, to the oft-debated issue of regulating information practices in the private sector.
Also on the legislative front, the Commissioner notes with great satisfaction the proclamation of Saskatchewan's *Freedom of Information and Protection of Privacy Act* and the intention of the government of British Columbia to proceed with the introduction of similar legislation. B.C. has engaged the services of Professor F. Murray Rankin as principal consultant, thereby ensuring the process will be favored with both enormous commitment and immense knowledge.

The extension of privacy protection to Canada's third most populous province means that more than 60 per cent of Canadians would enjoy the benefits of privacy oversight at the provincial level (joint Quebec and Ontario). The Commissioner is pleased to report that he has had consultations with officials of one other province now considering similar legislation.

All these developments must be regarded in a highly positive light. They constitute hard evidence that governments more and more are recognizing privacy not only as a right to which all citizens are entitled, but one which in the face of increasingly intrusive technology needs to be supported by its own set of laws and regulations.

The Private Sector: Voluntary Action

As previously mentioned, much of the Canadian banking industry now is covered by voluntary privacy codes. Following the promulgation of a model code by the Canadian Bankers Association, a number of the largest chartered banks have developed their own individual codes. While these codes differ in detail, and while they fall short of what the Commissioner would consider ideal, they share one important characteristic—the recognition that clients and customers have a vested interest in the fate of the personal information which they provide to the banks, and are entitled to some measure of consent and control.

As of this writing, for reasons mentioned earlier, these encouraging if less-than-perfect measures may be overtaken by the revised *Bank Act*. Even so, they provide an important starting point in what should be a joint government-industry effort. If *Bank Act* revisions do not occur, the Commissioner remains convinced that while the banks are to be commended for the progress made so far, their codes will still need to be strengthened.

Also heartening are signs of progress in the direct marketing field, which in recent years and as noted earlier has been the target of much public concern and complaint. The Commissioner commented previously and favorably upon a decision by the Canadian Direct Marketing Association to create a system by which Canadians could have their names removed from marketing lists held by the association's member companies. The association continues to work on an expanded code. It is unpublished as of this writing, but it is the fervent hope of the Commissioner that it will enlarge significantly the role of consumers, at least to the extent that prior consent becomes a condition of inclusion on such marketing lists.

Another promising initiative was undertaken during the year by the Canadian Standards Association (CSA) an organization whose primary responsibility is to ensure the safety and reliability of products marketed in Canada. CSA is most familiar to Canadians from its logo on products which conform to industry standards.

Shortly after the Commissioner's last annual report appeared with its news on the European draft privacy directives, the CSA contacted this office to offer a novel suggestion. CSA proposed formation of a committee to develop a model privacy code, one which would serve as a minimum national standard for private sector organizations handling personal information.

The CSA is ideally placed to develop such a code. It is an independent service organization of business, industry, labour, academia and regulators. This new proposal is a natural extension of the organization's involvement in international technology standards and its interest in technology's impact on consumers, business and industry.

A workable model code for the private sector would balance trade and business interests with consumers' inherent right to privacy. It would also demonstrate Canadian industry's commitment to the privacy principles contained in the OECD guidelines—and thus respond to the EC's requirement for "equivalent or adequate" protection.

The CSA code's committee (of which the office is a member) has drafted a proposal and has already received indications of interest and funding from AMEX, Readers' Digest, Bell Canada, Equifax and the federal departments of Consumer and Corporate Affairs and Communications.

If necessary, CSA will hire an experienced consultant to conduct research and work with the committee to develop the code. Once consensus is reached, the code will serve as the foundation, to be supported by various technical standards. It will become the cornerstone of a national compliance framework to help different business sectors establish privacy codes suitable for their particular environments.

The Commissioner strongly endorses CSA's approach and has committed the office's support. Private sector organizations interested in workable privacy solutions might find CSA's approach just what they are looking for.

Privacy At Work

Privacy in the workplace is an issue of rising concern, highlighted by the decision during the year of two major companies (Toronto-Dominion Bank and Exxon Canada) to introduce drug testing programs. Previous studies by the Office of the Privacy Commissioner have stressed the very limited utility of drug testing programs, and have concluded that the results to be gained do not justify the intrusive methods required. Developments in the past year suggest that the time has come to consider means by which individual privacy rights can be accommodated in areas of industrial activity which have special safety or other problems. It is not the Commissioner's view that no case can ever be made for testing programs; it is decidedly his view that such programs must meet demonstrated tests of both need and effectiveness.

Fine-tuning the Act

The *Privacy Act* has been part of the landscape for nine years, long enough for observers to form at least some interim judgments about its effectiveness. It is entitled to high marks.

The doctrine of fair information practices which is the heart of the *Privacy Act* has proved highly adaptable to a wide variety of situations in a rapidly-changing environment, and gives every sign of long life expectancy. Certainly, a better set of principles has yet to be devised.

The chief limitation of the Act is that it applies only to records in the custody of the Government of Canada and some of its agencies. Fair information practices have found their way into the laws of only a few other jurisdictions, and hardly at all into the private sector. So by far the largest part of personal information holdings in Canada continues to be unprotected.

Unless and until that situation changes, the *Privacy Act* will continue to be the most important piece of privacy legislation in the country, both for the immense holdings of personal information it covers in the Government of Canada, and for the benchmark against which data protection standards in other areas can be measured.

Thus, while the Act has weathered well, it needs to be constantly re-assessed, not in the sense of major overhaul but, if the phrase may be used, of "polishing the jewel". One comprehensive parliamentary review took place in 1986-87, as required by subsection 75(1) of the Act. But six years of added experience suggest it may be time for another.

Surprisingly though, we advise fine-tuning the Act's strengths: the definition of personal information (section 3), the fair information practices code (sections 4 to 8) and the access to personal records protocol (sections 12 to 28).

Redefining "personal information"

The *Privacy Act* architects could not have foreseen today's new technologies when they defined personal information. Advances in the science of genetics, for example, give added meaning to the words "information about an identifiable individual recorded in any form" (section 3—definition of personal information).

Locked in the smallest drop of body fluid or speck of tissue is a mountain of information that defines in minute detail the characteristics not only of individuals but also those of their forbears. Though paragraphs 3(b) and 3(d) refer to medical information and blood type, it is not clear that information recorded in biological samples about an identifiable individual falls within the scope of section 3. While it is clear the office would argue it does, any controversy regarding its inclusion could be eliminated by amending section 3. What is sought here is a clear statement that information contained in a genetic sample is personal information for purposes of the Act.

Some may argue that such an amendment is unnecessary tampering with an already elegant definition. But the genetic key is potentially so damaging to our privacy that a specific reference in the Act is needed.

Tightening up disclosures

Sections 7 and 8 of the Act are the foundation upon which are built our confidentiality rights. Its cornerstone is the principle of informed consent. Personal information cannot be used or disclosed without the concerned individual's knowledge and consent.

The *Privacy Act* demonstrates the truism that rules often need exceptions. Exceptions are necessary to strike a balance between an individual's right to confidentiality and the government's responsibility to manage the affairs of state. It is, for example, reasonable for personal information to be disclosed without consent to meet legal requirements or for criminal investigation purposes.

Curiously, one of the strengths of the legislation is contained in one such exception—paragraph 8(2)(m), disclosures in the public interest. The Act does not prevent public interest disclosures nor does it attempt to substitute detailed written rules for the reasoned and considered judgment of the head of an institution. It simply provides a transparent framework which ensures all interested parties are informed and that discretion regarding disclosure is properly exercised. The head of the institution who, after all, knows the records best, must balance the benefit to the public against the harm it may cause the individual.

However, most disclosures without consent do not require the head to exercise discretion. This may be delegated to staff. In this respect, the section is deficient. Staff should not be delegated the responsibility for consistent use disclosures; exchanges of information with foreign states or with the provinces; disclosures to investigative bodies, to Members of Parliament, to researchers, to auditors or to associations of aboriginal people. Since they are serious derogations from the prior consent principle, the head of the institutions should be required to decide on these disclosures.

This process might also resolve another difficulty with consistent use disclosures. Subsection 9(1) requires government agencies to notify the Privacy Commissioner of new consistent uses not recorded in *Info Source*—the personal information index. The office has received and assessed only 18 such notifications in its entire history. Our complaint and audit experience shows clearly that new consistent use disclosures are happening routinely without proper notification of the Commissioner. Surely higher level accountability would produce a more diligent application of all of the Act's requirements.

The Commissioner would welcome some fine-tuning of sections 7 and 8. The major flaw in the fair information practices code is its failure to provide a mechanism for an individual to prevent the release of personal information pending a determination of the propriety of its release. As previous annual reports have stated, it is an anomaly that individuals denied access to their personal information may go to court for review of the decision, but they cannot seek a review of a department's decision to disclose their personal information to third parties.

The *Access to Information Act* provides a mechanism for alerting third parties, such as corporations, whose sensitive commercial information may be shared. Yet, the *Privacy Act* provides no similar rights to individuals whose sensitive personal information may be disclosed. Does not personal information deserve protection from abuse that is at least the equal of that afforded corporate information?

True, in matters of national security or criminal investigations it may not be possible, or wise, to provide an individual with prior notice before disclosing sensitive personal information. These disclosures can be properly documented for the Privacy Commissioner's review.

Broadening the injury test

While the *Privacy Act* gives Canadians an impressive array of access rights, it also gives government institutions a vast—cynics might say limitless—arsenal of exempting provisions to defeat them. These exemptions are not unreasonable if they can be supported by clear, strong rationale. Most of them are. Who, for example, would want terrorists to learn that law enforcement agencies were hot on their trail, simply by applying for their records?

But some exemptions go too far. For example, government agencies can or must withhold personal information under sections 19, 22(1)(a) and 22(2) without demonstrating that release would cause some injury. These provisions concern, respectively, information obtained from other governments, law enforcement information, and information obtained by the RCMP while providing policing services to a province or municipality. Solicitor-client information (section 27) can also be withheld without a requirement to demonstrate that its disclosure would be harmful.

However, paragraph 22(1)(a) is certainly the most offensive. This section authorizes the government to deny access to personal information prepared "in the course of lawful investigations pertaining to the enforcement of any law of Canada or a province", provided the investigation was conducted by an "investigative body". There are nine such bodies listed in regulations to the *Privacy Act*. The exemption amounts to carte blanche to these bodies to deny Canadians access to their information for no reason whatever. No agency should be entitled to this kind of denial.

Generally this section has not been abused. The RCMP, for example, which has the right to use the exemption, rarely invokes it, preferring to use other sections of the Act. On the other hand, some cases demonstrate clearly how it can be misapplied.

One example concerned the Department of Consumer and Corporate Affairs (CCA). CCA's director of investigation and research investigated a complaint that the Parliamentary Press Gallery had violated federal competition rules when it denied an application for membership. CCA's investigation found no violation but, confronted with the complainant's subsequent privacy request for the opinions of Press Gallery members about his application, the department refused, taking refuge in paragraph 22(1)(a). Since CCA's investigation was complete, the Privacy Commissioner could find no valid basis for CCA denying the privacy request. However, the department was unyielding, and, given the blanket authority conferred by the section, he could do nothing more.

This kind of blanket exemption should be stricken from the Act. It has proved unnecessary even in such sensitive areas as police investigations. As it stands, it merely provides a convenient shield for bureaucrats not wanting to be troubled by the tiresome need to justify their decision. The following paragraph (22(1)(b)), with its injury test, provides a reasonable framework to allow government institutions to effectively manage their programs.

The scope of this exemption explains the Commissioner's reluctance to applaud additions to the list of investigative bodies. During the year, the Commissioner learned that three new bodies were being considered. The quarrel is not with the particular bodies being considered but rather with the concept of any investigative bodies at all. Other exemptions—subject to an injury test—provide all the latitude needed. The Commissioner's office is now part of a working group examining the exemption, its uses and some options for the future.

"Catch 22"

One final preoccupation about the Act needs addressing in this report.

Section 16 allows an institution to refuse to either confirm or deny the existence of personal information. To most of us at least, other exemptions provide a more than sufficient limitation to the general right of access. Section 16, though, goes far beyond the mere refusal to provide access.

The doctrine of refusing to confirm or deny is ingrained in Canadian security and policing psyches, and it would seem that section 16 is its statutory embodiment. As distasteful as the notion is in a free and democratic society, it may be necessary for us to tolerate its use in order to achieve a public good. But invoking this section with any exempting provision other than those concerned with security and policing (sections 21 and 22), would surely constitute an unacceptable encroachment on an already too highly encumbered and fragile right of access. The Act should be amended to limit this authority to national security and criminal investigations.

The threat to our privacy rights is compounded because though the Privacy Commissioner may investigate complaints about this section, he cannot reveal any information or even that there is no information!

Should the Privacy Commissioner be unable to resolve the complaint, he faces Catch 22. Simply by referring the matter to Federal Court he runs the risk of revealing the existence of information, thus breaching his own Act. The Act needs a mechanism to enable the Commissioner to refer these complaints to the Courts for adjudication.

Genetic Testing

It is easy to overlook the privacy implications of technologies many of us do not yet fully understand. Nowhere does this pose a greater danger than with genetic testing.

Advances in genetic technology promise to unravel medical mysteries, thus preventing many diseases and allowing treatment of others. The technology can already identify many genetic traits or disorders and, occasionally, accurately predict our genetic destinies. This news is good. But there is also the inevitable dark side. Genes can reveal deep secrets about individuals' physical and psychological being—secrets they may not want others to know, or may not want to know themselves. Stripping away the human being's very essence to the twisted strands of DNA molecules—the personal genetic building blocks — is an assault on privacy that few may want to endure.

Do governments or other organizations have a right to acquire personal genetic information "for the public good", with or without consent? Or should individuals be able to protect their genes from inspection by either the state or the private sector?

This year the office completed its report, *Genetic Testing and Privacy*, the third in a trilogy on biomedical testing. (The first two dealt with HIV/AIDS and drug testing.) The latest report examines the issues flowing from the rapid development of genetic testing technology, including several present or potential uses. These tests could be designed to select genetically fit employees or monitor the effects of workplace hazards on their health; determine eligibility for such benefits or services as insurance; diagnose or predict medical conditions during regular medical care or reproduction (pre-conception, prenatal and neonatal), and provide more accurate forensic evidence in criminal investigations.

To date, genetic testing in Canada appears to have been limited to three fields — reproductive technology, regular medical care, and criminal investigations. Still, the advent of cheaper, more informative tests will almost certainly stimulate further interest in testing. Governments will not be the only intruders. Private sector interests, such as employers and insurers, will become increasingly enthusiastic about the supposed ability of genetic testing to give them a competitive edge.

Governments may be tempted to override serious ethical concerns and apply genetic knowledge to promote eugenics. Certainly today's world is not free from pressures to thus create "better societies". In the private sector, genetics could be used to identify genetically "inferior" individuals. For these unfortunate members of the genetic "underclass", access to employment or services could be severely impaired.

In both environments—government and private sector—people could find genetic traits over which they have no control determining how they will be permitted to lead their lives, with little concern shown for the person behind the genes.

This office was chilled by the potential growth in the number and types of intrusions that may ensue as genetic technology advances. Accordingly, the report recommends against mandatory (and, in some cases, voluntary) genetic testing in several situations. It also calls on the federal government to study the extent of genetic testing in Canada, and the likely future uses of this technology.

Prominent recommendations of the report are:

- every person should have a reasonable expectation of genetic privacy;

- governments should collect personal genetic information only if specific statutory authority permits;

- neither government nor the private sector should compel persons to learn their genetic traits or disorders;

- employers should not require genetic testing in employment, whether to identify undesirable genetic traits in employees or applicants, or to identify genetic changes due to workplace exposures; only true voluntary testing would be allowed;

- service or benefit providers should not be permitted to use mandatory genetic testing to determine a person's eligibility for services or benefits;

- governments should not collect personal genetic information relating to the reproductive process;

- governments should not collect personal genetic information relating to ordinary medical care;

- governments should restrict forensic DNA analysis in criminal investigations to identifying offenders or exonerating suspects;

- governments should not establish personally identifiable genetic databases or banks of genetic materials from the general population for crime control.

The report merely scratches the surface of genetic testing. The Commissioner hopes it will stimulate thought and action before powerful public or private sector interests transform us all from human beings into the mere sum of our genetic parts.

A Year in the Privacy Trenches

Telecommunications toys—playing with privacy

Readers of these reports may recall the former Privacy Commissioner's concern about the privacy threats in new telecommunications technology (1989-90 report, p. 26). The Commissioner cited Bell Canada's new Call Management Services (CMS)—and Caller ID in particular. The CRTC has since approved Bell Canada's service and similar ones are now available from most telephone companies.

Caller ID is just one element of the new telephone technology. Many new phone services are not features of improved telephone sets but the product of powerful computers which handle telephone switching operations. However, users do need specially equipped telephones to allow them to see and record the caller's phone number before picking up the handset.

Seeing the caller's number before answering may provide protection against harassing calls. But it also trades away the rights of others who have an equally legitimate desire to avoid having their phone number known or recorded.

This desire—or need—for anonymity is obvious for those calling crisis hot lines or for volunteers who often return calls from home. Many professionals—from psychiatrists to probation officers, from politicians to undercover police officers—may now be unable to call from home, not wanting their numbers displayed and recorded.

Many are also concerned about commercial use of their phone numbers. Anyone calling a business with a casual inquiry now courts the risk of having their number recorded, only to be called back for marketing purposes. Reverse directories (which list subscribers sequentially by phone number) can then link the number to a person and address.

Trading away everone's privacy is a heavy cost for CMS' few benefits. Charging subscribers to **prevent** the display of their numbers means privacy is for sale and not everyone will be able to afford it.

These concerns are well-founded and workable solutions are elusive. CMS can vary from one phone company to another, making privacy protections a patchwork. Some companies allow callers to block the number display for all calls on their line—or just selected calls—but at a cost. Some charge nothing to block. Others offer a form of encryption which scrambles the number. Nearly all companies offer a solution for women's shelters.

One recent CMS decision comes from the Manitoba Public Utilities Board. The board approved Manitoba Telephone System's application for a trial run, providing that all subscribers benefitted from free call blocking. The board also demanded free line blocking for shelters and individual victims of abuse. However, the board did not approve Call Return—the option which traps the numbers of unanswered incoming calls and displays them later on command.

Of broader significance is the CRTC's recent announcement–well after the end of our reporting year–that phone companies under its jurisdiction must offer free per-call blocking.

Canada is not alone in its struggle to find appropriate solutions for technological advances. In the United States, the debate has raged since New Jersey introduced the service in 1987—a debate involving public utility commissions, state and federal legislatures and even the courts.

And the solutions range from New Jersey's, which offers no blocking at all, to Pennsylvania where CMS has been ruled illegal since it offends the state wiretap law.

Texas proposes that customers pay if they want to display and, most recently, an administrative law judge in California proposed that the state utilities commission prohibit Caller ID because it is not in the public interest and violates both the state and federal constitutional right to privacy.

Still other states offer free per-call blocking, pay-per-line, free per-call **and** per-line blocking. At the height of the debate, one company even offered a service to automatically refuse blocked calls. The options are dizzying.

The debate has focussed public attention on the privacy issue. Probably more disturbing is the knowledge that these services are only the beginning—an early feature of the ever-increasing intelligent network system. This system will soon offer personal communication networks with a lifetime personal phone number, dial-up services and picturephones. The technology is evolving so fast that neither engineers nor policy makers have time to consider the social impacts. Each new development affects or overrides the privacy protections so laboriously erected to defend against the last one.

Obviously the Privacy Commissioner's small office cannot keep abreast of each new technical marvel; it lacks the expertise and resources. Nevertheless, the Commissioner is eager to find enduring and workable solutions.

The New York State approach has substantial appeal. That state's public service commission took a broad policy approach to telecommunications privacy, approving eight privacy principles. They state, for example, that telecommunications companies should recognize clients' privacy explicitly and that customers should not pay extra to preserve their privacy status quo. Customers should be told of any proposed use of their information and be able to give informed consent to any further uses.

The office and the Department of Communications are both examining the broad issue of telecommunications impact on privacy and considering some remedies.

New Telecommunications Act

A step in the right direction may be the initiative in the proposed *Telecommunications Act* in which Parliament recognizes the privacy impact in telecommunications technology. The act includes as a policy objective

> " ...to respond to the economic and social requirements of users of telecommunications services, including the protection of the privacy of individuals. ..."

This act also allows the government and the CRTC to block such intrusions as unsolicited phone calls and junk faxes.

The office intends to monitor passage of this bill through the House to help ensure that the privacy protections are not eroded. At issue is whether its provisions go far enough. Either the act or its regulations should outline the privacy standards which telecommunications services must meet.

This year's SINs

Born without SIN

Resistance to demands for the Social Insurance Number (SIN) took an unusual turn this year when a Prince Edward Island couple refused to apply for a SIN for their newborn baby.

PEI's vital statistics department requires all newborns to be assigned a SIN for the province to use as identification numbers for its Health Service Payment Plan. The couple asked for an exemption and were denied. The health department responded by refusing all claims for the baby's medical care because she did not have a SIN.

The couple has taken the case to court, arguing that requiring the baby to have a SIN (and denying the medical claims) offends several provisions of the *Canadian Charter of Rights and Freedoms*. The parents maintain that their daughter has no legal obligation to obtain a SIN until she begins insurable employment. They argue further that denying the medical claims offends *Charter* protections against unreasonable search and seizure and denies the baby's right to equal benefit of the law, and requiring a baby to have a SIN breaches an individual's reasonable expectation of privacy.

The case is interesting to this office, although well outside the *Privacy Act*. But it does raise an important privacy question: what program or activity of Employment and Immigration Canada (the department responsible for issuing SINs) allows it to issue the numbers to newborns?

SINs were created for unemployment insurance and Canada Pension Plan, and later authorized for use by Revenue Canada for individual income tax reporting. Recent federal government policy—applauded by the Privacy Commissioner—has reined in many unrelated federal government uses of the numbers. However, apparently EIC still relies on a 1970 federal-provincial agreement concluded well before any federal privacy protection was in place.

The Commissioner has asked Employment and Immigration to identify a direct relationship between assigning SINs for birth registration and EIC programs. If none can be shown, he will urge EIC to reconsider its arrangement with PEI in light of both the *Privacy Act* and the federal government's policy to restrict SIN use to a short list of social programs.

Casting the first stone—
renumbering the public service

One significant impact of the federal policy to restrict its own use of SIN is the need to re-number some 310,000 public servants, members of the military and RCMP.

Supply and Services Canada (which controls the pay and records data bases) will begin assigning new Personal Record Identifiers (PINs) by January 1993. Each employee will receive two numbers: the PIN and a second number to be given to third parties such as banks, insurance companies and the employees' unions. This second number will ensure that employees' PINs remain private but allow the employer to link third party transactions to the correct employee.

There remains some confusion about what constitutes a proper request for a person's SIN. For example, the Public Service Commission's language testing programs still ask employees to volunteer their SIN and public service unions continue to use SINs for membership purposes. These are legitimate requests. But once the renumbering is completed, the Commissioner urges federal employees to keep their new PIN to themselves.

SIN or else

The Commissioner's office was alerted to what seemed to be an unnecessary use of SIN in Employment and Immigration Canada's new automated Job Information Bank in St. John's, Newfoundland. The pilot project allowed job seekers to scan a computerized listing of available positions and select those that matched their interests and skills. The system gives applicants greater opportunity and frees up EIC staff for other duties.

However, a caller complained that he could not even look at the list without first providing his SIN. Since any casual passer-by can scan the paper notices of jobs available, he thought demanding a SIN for a computer listing was excessive and—since he was not claiming unemployment insurance—unneccessary.

Apparently EIC asked for the SIN to measure both the effectiveness of the system and its ability to place UI claimants. Responding to the office's enquiries, EIC acknowledged that the system should also accommodate non-UI claimants.

The system has now been modified. The opening screen advises users that access to the system is unrestricted. Those receiving unemployment insurance have the option of entering their SINs so that the Canada Employment Centre has a record of their job search. This change will become part of the new nationwide job-bank system.

Technology update

Last year the Commissioner reported on Employment and Immigration Canada's (EIC) plans to harness new information technology to handle the department's huge client load. EIC had pilot projects underway using smart cards and an automated telephone answering service (AVRES).

EIC is not the only federal department considering using new information technology to improve service. Veterans' Affairs has already tested smart cards as a method of improving its delivery and billing of prescription drugs to veterans. Revenue Canada is looking at the possibility of having travellers use the cards to declare goods or pay fees at customs points.

Several departments are jointly developing smart cards which would allow remote access to government computers. This would permit someone working at a home personal computer to communicate with a government agency's computer over the telephone.

As with much of the new communication technology, there are privacy implications.

The smart card is like a conventional bank or credit card—but with an essential difference. Smart cards are imbedded with an integrated circuit chip which gives the card intelligence for processing and memory for storing data. Chips and digitized information also make it possible for the cards to carry an invisible photograph or even a fingerprint of the bearer. The cards could be used to provide banking, telephone and medical services, giving the user access to a network of computers.

Privacy needs

Clearly smart cards are an important technical advance which can improve service to clients and control costs for departments—particularly those like EIC which must track, credit deductions for and pay benefits to such large numbers.

Yet government agencies and their clients should be able to enjoy the benefits of progress without sacrificing individuals' control over their personal information. In effect smart cards could become that universal identity card that North Americans so fiercely resist. Their development invites a profound shift in the relationship between the individual and the state.

This can be avoided, first, by making the systems transparent to the clients. Card bearers must know their inherent rights when using the card, what information the card contains, how it will be used, and what risks that use implies.

Individuals should be free to refuse the card without jeopardizing their access to the service. And similarly, holding a card should not confer advantages unavailable to those who opt out.

Finally, the systems and their participants must respect both privacy laws and basic ethical principles on collection, handling and disclosure of personal data.

Because of the Commissioner's concern about the security aspects of the pilot projects, his staff were invited to join two federal government working groups: one dealing with applications of the technology and the other developing standards for remote access to computer systems.

The applications group—whose ultimate goal is to establish standards and guidelines for all government smart card applications—will identify how government might use the cards and the framework in which they should operate. Its membership includes such federal agencies as Health and Welfare Canada, Supply and Services Canada, the RCMP and Veterans' Affairs, as well as the Quebec and Ontario health ministries.

The office is also a member of a special interest group working on the development of remote access to computer systems. Since many government agencies have a common interest in access, they are sharing research and development costs and contributing to shared standards.

The AVRES Project

Last year's report (p.53) described a privacy flaw in EIC's automated telephone inquiry system being tested in Quebec City. The story ended unsatisfactorily since the project seemed too far advanced to change. However, EIC has re-written the ending and the Commissioner could not be more pleased.

The system allowed claimants with touch-tone telephones to call into a computer for routine information about their own unemployment insurance claims. For example, a caller could confirm that his or her claim had been accepted and when benefits would begin. Callers identified themselves by their Social Insurance Number (SIN) and birthdate. The office heard about the service when a local radio station questioned this use of SIN.

There was no question that EIC could use SINs to identify UI claimants—the numbers were devised for this purpose. But the Commissioner was concerned about the lack of security of the SIN-birthdate combination. The office discussed the problem with EIC staff who agreed that both pieces of personal data are widely available and therefore not a secure access code. However, the test project had already expanded to London and Peterborough and it seemed too late for changes.

Nevertheless, aware of the Commissioner's concern, EIC systems designers used the Peterborough project to test a new four-digit telephone access code similar to a bank number.

Apparently the test was successful and the new code will be a feature of the national program. EIC will assign claimants the number to identify themselves when making telephone inquiries. Claimants may also choose their own numbers.

The Commissioner applauds EIC's quick response and its sensitivity to client security.

Data Matching

Probably the most important data matching news this year is what did not happen—apparently data matching did not happen. The Commissioner received just three notifications during the entire year—all from Agriculture Canada.

The Commissioner wishes not to appear suspicious. Yet it would be credulous to accept that of more than 150 federal agencies subject to the government's data matching policy, only one began any new matches of discrete sets of files during 1991-92.

The matching policy restricts linkages between computer data bases that could produce detailed dossiers—or "super files" on individuals. It also requires federal agencies to submit matching proposals to the Commissioner 60 days in advance. He then assesses the match against a set of criteria and acts as an advocate for the subjects of the files. The intent is to prevent government efficiency from trampling individuals' personal information rights.

The policy, while admirable, may not be working. Only 22 federal agencies describe anything remotely resembling a data match in their listings in *Info Source*—the federal information directory. Some departments couch matches under more benign headings like "use" or "disclosure". And others only recognize a match when it links with data from an outside agency, contrary to the policy which also controls matches of different program files within an agency.

Everything the Commissioner has seen leads him to conclude that computer data matching is common in government—particularly with social programs, law enforcement and intelligence operations and the criminal justice system. Do government staff recognize a data match? Are they unaware of the policy? Or do they simply see the policy as a nuisance to be avoided?

The Commissioner urges the Treasury Board to investigate. In the meantime, the Commissioner's compliance auditing teams have added data matches to their list of audit criteria.

Agriculture Matches

In fairness, Agriculture Canada has been scrupulous in observing the data matching policy. Its first notice advised that the new *Farm Income Protection Act* would allow Agriculture to match farmers' information from the income stabilization account with income information from Revenue Canada.

The match will ensure that the benefits farmers receive from these programs are based on correct information about their revenue, expenses and production. The act gives Agriculture legal authority for the match and allows it to use the Social Insurance Number.

Garnishees for Family Support: Agriculture also advised the Commissioner that it would match information from the Western Grain Stabilization Program with the Department of Justice to allow garnishee of program payments from farmers who had defaulted on their family support. In fact, the submission was unnecessary because Parliament had passed a regulation under the *Family Orders Agreements Enforcement Assistance Act* authorizing deductions from the stabilization program.

More Information Needed: Finally, the Office was notified of a match between Farm Debt Review Board files and Quebec agriculture department records. The match supports a new program to subsidize beef feed lot operators and to mediate with farmers' creditors. The Office has not received sufficient detail to assess this match.

Complaints Directorate

The office received 1,402 new complaints this year compared with 1,239 last year—an increase of 13 per cent. This increase is consistent with the pattern established since the office opened in 1983. Not consistent is the drop in the number of completed cases—782 cases were closed, 269 of which were well-founded, 448 not well-founded and 65 discontinued.

The 1991 Census

During the past year, one issue has consumed considerable time—investigating 34 complaints against the 1991 census. Several complainants were concerned about Statistics Canada's collection of personal information and had refused to respond to census questions they considered an unacceptable invasion of their privacy.

Others cited the guarantee (or lack) of confidentiality of their census responses. The most frequent complaint was that census workers who gathered the results were neighbours or acquaintances of the complainants. Complainants believed that their completed questionnaires would be sent directly to Statistics Canada in Ottawa to be reviewed by some anonymous bureaucrat, not by someone from their neighbourhood. The investigation is now in its final stages and its results will soon be shared with Statistics Canada.

This is the first time this office has undertaken such a complicated and time-consuming investigation, and it has taken its toll. The nearly six months spent by three senior privacy officers who spearheaded the investigation took time away from other cases. This is the main reason that the number of completed cases is lower than last year. Staff turnover (and subsequent training) has also contributed, thus exacerbating a growing backlog.

A New CPIC Policy

The Canadian Police Information Centre (CPIC) continues to be the target of complaints and inquiries about the collection, use and disclosure of personal information held in its databases. CPIC is a collection of police databases, federally funded and administered by the RCMP. However, it is governed by an advisory committee of major municipal and provincial police forces who contribute and have access to the information.

We often hear from individuals who cannot get access to their own information in CPIC because various police forces cannot disclose information contributed by others. For example, CPIC may not disclose personal information contributed to it by the Ottawa City Police.

This office has discussed its concerns about CPIC's administration in earlier reports and recommended that the RCMP consult other CPIC users about introducing voluntary privacy controls over its databases. This would provide comprehensive protection for CPIC's collection, use and disclosure of personal information, and allow individuals to access and correct their personal data.

Congratulations are in order. CPIC approved and implemented a CPIC Code of Ethics in November 1991, one which generally addresses the Commissioner's concerns—particularly those dealing with access rights. It entitles individuals to request access to their personal information maintained on CPIC and to correct it, when necessary.

Top Ten

Last year, for the first time the office listed its top ten clients—a group which accounted for 80 per cent of the total caseload. Eight of those ten departments made the list again this year: Correctional Service Canada (CSC), Canada Post Corporation, Employment and Immigration Canada, Revenue Canada-Taxation, National Defence, Canadian Security Intelligence Service(CSIS), RCMP and National Archives.

Joining the top ten is the Immigration and Refugee Board (IRB) with 68 complaints received—the first privacy complaints received against IRB. However, 67 of those were made by one person, including 33 time limit complaints which were considered well-founded. Investigation of the 33 access complaints continues.

Completed Complaints by Grounds and Results

	Disposition				
Grounds	Well-founded	Well-founded/ Resolved	Not Well-founded	Discontinued	TOTAL
Access	5	102	260	41	408
Access	5	102	260	41	408
Correction/Notation	0	0	29	0	29
Index	0	0	3	0	3
Language	0	2	0	0	2
Privacy	5	12	82	13	112
Collection	1	2	35	4	42
Retention & Disposal	1	1	8	4	14
Use & Disclosure	3	9	51	3	66
Time Limits	142	3	89	11	245
Time Limits	138	3	90	11	242
Extension Notice	4	0	0	0	10
TOTAL	152	117	448	65	782

Another significant increase occurred at Revenue Canada-Customs and Excise. Their 72 complaints constitute a five-fold increase over last year's figures.

Last year's report applauded CSC for its efforts to conquer its delay problem. Unfortunately CSC's delay complaints more than tripled this year—160 (compared with 50 last year). These delays account for 34 per cent of the year's time limit complaints. However, this warrants an explanation. CSC has changed the way it processes information about inmates that it receives from provincial and municipal governments and police forces. CSC routinely used to exempt information received in confidence from another government. However, after years of urging from this office, CSC now asks the originator whether it will agree to disclose.

This causes delays for applicants. With heavy caseload and shrinking resources, CSC has to choose between two evils: providing a less than complete response in time—or go the extra mile, risk exceeding the time limits but provide the applicant more information.

Other departments also continue struggling to meet time limits: National Archives, Revenue Canada-Taxation and National Defence.

Toward the end of the reporting year, the office changed the way it reported time limits complaints. Frequently, complainants question departments' claims of a time extension either to consult other organizations or because operational requirements prevent them from responding within 30 days. The office did not count the number of complaints specifically questioning the notice. But time limits complaints have now been divided into two categories: time limits and extension notices. The change acknowledges the distinction between the two issues. It also identifies departments which continue to neglect their responsibilities to respond in time.

At a time of government restraint it is difficult to chastise departments for not respecting the time limits. Budgets and staff have been slashed in most government departments with the result that service to the public suffers.

While the number of time limits and access complaints received increased by 31 per cent from 855 last year to 1118 in 91-92—the number of complaints about improper collection, use and disclosure dropped by 26 per cent—from 384 in 90-91 to 284 in 91-92.

How Institutions Measured Up

The RCMP continues to carry the banner for maintaining its high regard for the letter and spirit of the Act. Only one of its complaints was well-founded, resolved; 40 were not well-founded, while three were discontinued. CSIS too must be commended; of the 56 complaints completed last year, only five were considered well-founded, and all were resolved.

Last year CSC had the highest ratio of well-founded complaints, with EIC, Taxation and DND not far behind. This year, despite continuing to head the list of complaints received (a total of 287), only 27 per cent of all CSC's complaints were well-founded. Approximately one-half of the complaints against EIC and Taxation, and 32 per cent against DND were well-founded.

This year's number of discontinued findings is high—65 represents eight per cent of completed cases. However, the majority were discontinued when the office's initial notice to the departments prompted them to resolve the problem. Of course, that's what the ombudsman's role is all about—resolving problems, not counting complaints.

Top Ten Departments by Complaints Received

		Grounds		
Department	TOTAL	Access	Time Limits	Other
Correctional Service Canada	287	92	160	35
Canada Post Corporation	148	101	8	39
Employment and Immigration Canada	135	72	26	37
Revenue Canada, Taxation	107	27	59	21
National Defence	90	20	63	16
Canadian Security Intelligence Service	87	77	10	0
Royal Canadian Mounted Police	84	67	4	13
Revenue Canada, Customs & Excise	72	29	31	12
Immigration and Refugee Board	66	33	33	2
National Archives of Canada	47	14	23	10
OTHER	273	119	55	99
TOTAL	1,452	681	487	394

Proposals for New Exempt Banks

The office was consulted twice during the year on proposals to create new exempt banks. The RCMP advised the Commissioner that it intended to seek Cabinet approval to create an exempt bank for its National Security Investigation Records. CSIS also notified the Commissioner of its proposal to seek an exempt bank for its Investigation Records.

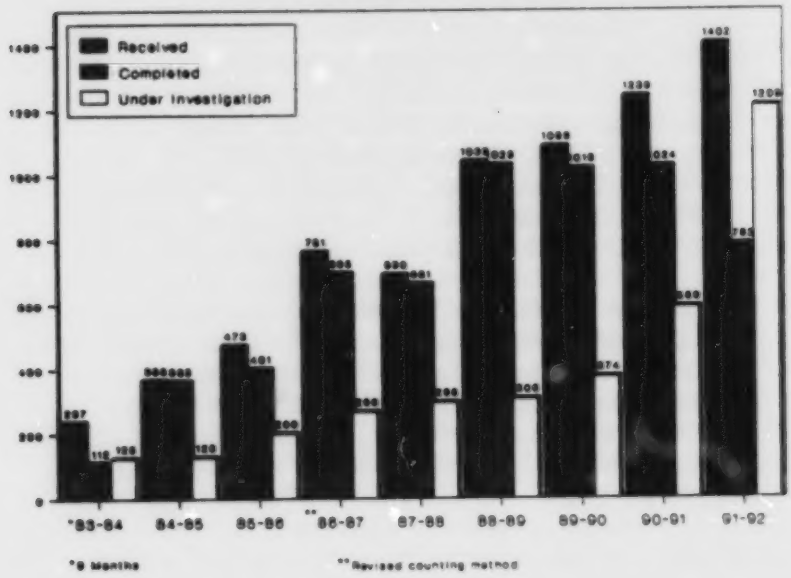
A staff review of both banks determined that they consist predominantly of personal information obtained or prepared during criminal investigations or whose release could damage the conduct of Canada's international affairs or defence (sections 21 and 22 of the *Privacy Act*). The Commissioner would not comment personally on the validity of the exemptions in order to avoid any conflict of interest should he receive a complaint about information contained in the files.

The Constant Plea for More Resources

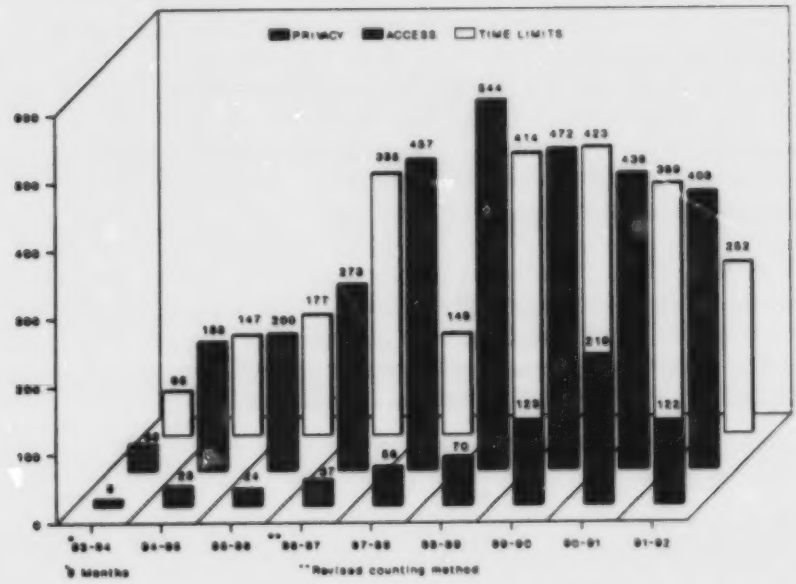
The 13 per cent increase in new complaints has put the office behind by almost a full year's caseload—1209 cases pending at year end. As predicted in last year's annual report, the backlog increased investigators' workloads to 200 each. Thus clients are now kept waiting sometimes months longer than they should to receive the Commissioner's finding.

Treasury Board allotted the office two additional person years to hire more privacy officers. But if new complaints continue to arrive at last year's pace, the office faces the spectre of more than 2000 open cases. This risks becoming unmanageable.

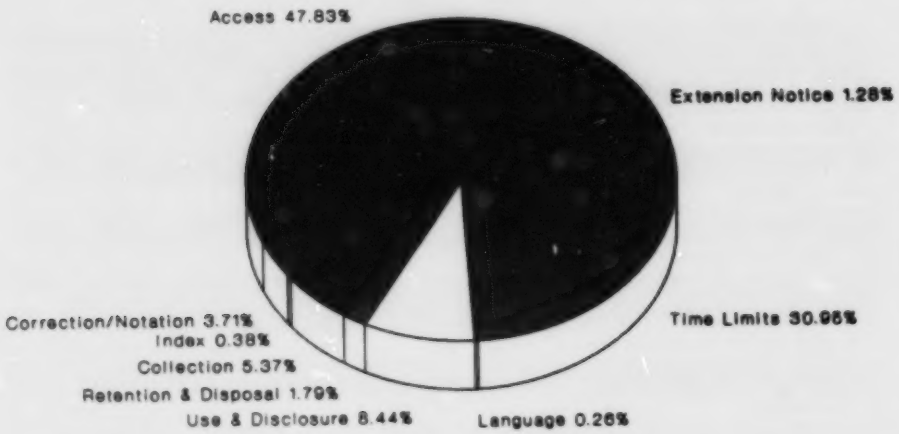
Completed Complaints 1983-92



Completed Complaints and Grounds 1983-92



Complaints Completed by Grounds 1991-91



Origin of Completed Complaints

Newfoundland	4
Prince Edward Island	20
Nova Scotia	17
New Brunswick	226
Quebec	30
National Capital Region Quebec	144
National Capital Region Ontario	2
Ontario	762
Manitoba	
Saskatchewan	
Alberta	
British Columbia	
Northwest Territories	
Yukon	
Outside Canada	
TOTAL	

Completed Complaints by Department and Result

Department		Dispositions			
		[illegible]	[illegible] Resolved	Not Well-Founded	Discontinued
Agriculture Canada	3	0	2	1	0
Atomic Energy Control Board	1	0	1	0	0
Bank of Canada	2	0	1	1	0
Canada Post Corporation	67	2	9	55	1
Canadian Human Rights Commission	2	0	0	2	0
Canadian Radio-Television and Telecommunications Commission	1	0	0	1	0
Canadian Security Intelligence Service	56	0	5	42	9
Commissioner of Official Languages	1	0	1	0	0
Communications	1	0	0	1	0
Consumer and Corporate Affairs Canada	9	0	0	3	6
Correctional Service Canada	130	10	25	76	19
Employment and Immigration Canada	71	11	22	30	8
External Affairs Canada	13	0	7	6	0
Farm Credit Corporation Canada	1	0	1	0	0
Fisheries and Oceans	10	1	1	8	0
Forestry Canada	1	0	0	1	0
Health and Welfare Canada	7	2	0	5	0
Immigration and Refugee Board	34	33	0	0	1
Indian and Northern Affairs Canada	11	7	0	4	0
Justice Canada	8	0	1	7	0
Labour Canada	3	2	0	1	0

Completed Complaints by Department and Result

Department	Total	[illegible]	[illegible]	[illegible]	[illegible]
National Archives of Canada	10	2	1	6	1
National Capital Commission	1	0	0	1	0
National Defence	110	25	10	65	10
National Parole Board	35	6	8	20	1
Office of the Superintendant of Financial Institutions Canada	3	2	1	0	0
Privy Council Office	1	0	0	1	0
Public Service Commission of Canada	6	0	3	2	1
Public Service Staff Relations Board	1	0	0	1	0
Public Works Canada	2	0	0	2	0
Revenue Canada, Customs and Excise	25	15	4	5	1
Revenue Canada, Taxation	67	31	4	31	1
Royal Canadian Mint	1	0	0	1	0
Royal Canadian Mounted Police	44	0	1	40	3
Secretary of State of Canada	2	0	0	1	1
Solicitor General Canada	5	0	0	5	0
Statistics Canada	3	0	0	1	2
Supply and Services Canada	7	1	0	6	0
Transport Canada	20	2	12	6	0
Veterans Affairs Canada	7	0	0	7	0
TOTAL	752	182	117	443	65

Some Cases

CPIC limits AIDS identifiers

A group of community organizations in Vancouver asked the Privacy Commissioner to look into allegations that Canadian Police Information Centre (CPIC) databases identified individuals as HIV positive.

Although no one could point the finger at a specific incident—and the office's jurisdiction over CPIC is questionable—the Commissioner decided to inquire informally.

The RCMP (which administers CPIC) explained that individual CPIC files could contain a "C" flag to indicate that the person has a contagious disease. The flag helps police find individuals with communicable diseases who have escaped from penitentiaries or wandered away from hospitals. It also helps police inform those who may have been exposed to disease.

The CPIC advisory committee asked for a legal opinion on identifying HIV/AIDS carriers. As a result, CPIC policy now forbids identification of carriers unless they have threatened to transmit the condition using physical violence or, for example, if a carrier has violated the public health act by willfully spreading the virus.

CPIC contacted all CPIC users to explain the new policy and a subsequent audit identified 96 "C" entries (not necessarily HIV/AIDS). Since then CPIC has reminded users and done yet another audit which found fewer than 40 "C" files remaining—all for *bona fide* law enforcement reasons.

Finally, an RCMP member and the privacy investigator met the coalition members in Vancouver to brief them and answer questions. The coalition appeared satisfied with the outcome. The Commissioner is particularly grateful that CPIC and the RCMP were willing to listen and respond to the group's real concerns.

Respondent should see entire file

A complaint about the Public Service Commission's handling of an application to see a personal harassment investigation file revealed what seemed to be inconsistent treatment.

The applicant (the respondent in the harassment case) was given only those parts of the file that PSC considered his personal information. The investigation revealed that PSC processes harassment files differently, depending on who is the applicant. When the applicant is also the complainant, PSC considers the entire file that individual's personal information and discloses everything except that which may be exempted under the *Privacy Act*.

However, when the applicant is someone else—for example, witnesses or the respondent—PSC processes only those records considered to be the applicant's personal information.

The privacy investigator considered that since the applicant was also the alleged harasser and lone respondent—and the entire file dealt with the investigation of a complaint against him—PSC should process the entire file.

PSC officials have agreed that when the respondent is an individual (rather than the department), it will process privacy applications from both complainants and respondents in the same way. This means that all information on the PSC investigation file will be disclosed unless it may be exempted under other provisions.

Since the applicant had not been denied access to any of his own personal information, his complaint was not well-founded. However, his complaint prompted PSC to disclose the remainder of the file which did not qualify for exemption and to change its processing methodology.

New spouses get equal treatment

An employee of the Communications Security Establishment (CSE) told his supervisors of his pending marriage, a requirement of all federal employees holding a secret or top secret security clearance. The employee provided his bride's name, birthdate, address and name of present employer—as required by the government's Personnel Security Clearance Questionnaire.

However, CSE also requested details of the new spouse's residence and employment from the previous five years. At that point, the woman complained to the Privacy Commissioner that CSE's demands for more information invaded her privacy. She also held that CSE should have asked her directly for the information and not collect it from a third party.

The investigation revealed that CSE's policy on security reliability checks was inconsistent with most other federal government departments which rely on the information on the employee's security questionnaire. As well, new CSE employees are not required to provide the more detailed information about spouses. Only established employees who change their marital status must provide their new mate's residence and employment history.

DND was the only other department found to demand this supplementary information in similar circumstances, asking for details of residence and employment over the previous ten years.

Without question, details of relatives' personal history is needed to conduct background checks on those in a position to influence employees with access to national security secrets. However, it was difficult to understand why CSE needed more personal history of new mates of its established employees than of spouses of new employees.

CSE officials were persuaded to bring their policy in line with other departments. Ironically, before the Commissioner's office pursued the matter with DND, its policy had already been amended.

The complaint was well-founded but resolved.

Bulletin boards no place for grievance responses

A National Defence employee complained to the Commissioner that his supervisor had posted on a bulletin board DND's response to his formal grievance about smoking in the workplace. The department's letter included his name, address and comments on DND's policing of its anti-smoking policy.

The investigation found that indeed the letter had been posted in the room where the complainant worked, in full view of other civilian and military employees. Apparently a manager had told the man's supervisor to post the letter as a reminder to personnel to comply with the anti-smoking policy.

Following the investigation, DND agreed that the personal letter should never have been the mechanism for reminding employees not to smoke in DND buildings. DND has ensured this will not happen again.

The Commissioner considered the complaint well-founded.

Employees' personal papers not for disclosure

During its investigation of a harassment complaint Revenue Canada-Customs searched the office of an employee it suspected of writing an anonymous note found on a colleague's desk. Revenue Canada investigators photocopied the employee's personal phone directory and took documents from his personal files to have analyzed by handwriting experts.

Discovering this, the employee complained to the Privacy Commissioner that Revenue Canada had improperly disclosed his personal information. The Commissioner's investigation established that personal documents had been taken; used during the harassment investigation, and disclosed outside the department without the complainant's consent.

The documents included employee benefit statements—including some medical information—and his completed personal record form which lists education, previous employment, personal references and identifies family members, their occupations and addresses. The Commissioner concluded that the use of this type of personal documentation during an internal investigation could hardly be "consistent" with the original collection purpose. He considered the complaint well-founded.

Revenue Canada-Customs has apologized to the complainant for disclosing the documents and has amended its investigation manual to prevent investigators from using such personal information without the individual's consent.

Anonymous tipster not EIC

A complainant alleged that Employment and Immigration Canada (EIC) had disclosed to his ex-wife information about his earnings from his unemployment insurance file. She then used this information in a court application to increase his support payments.

The investigator interviewed the two EIC employees who dealt with the complainant, both of whom denied disclosing any of his personal information to any unauthorized persons. The ex-wife and her current husband were also interviewed. They too denied having obtained the information from EIC, saying that the tip-off came from an anonymous caller.

The Commissioner concluded that there was no evidence to support the man's allegation that EIC staff were the source of the information and he dismissed the complaint.

Complainant revealed identity himself

A man complained to the Commissioner that Employment and Immigration Canada (EIC) officials had identified him to an EIC-funded organization as the applicant seeking information about it under the *Access to Information Act*. The complainant correctly observed that identifying him as the applicant was an improper disclosure of personal information.

The investigation established that the complainant had had a dispute with the managers of the organization which provides on-the-job training to otherwise unemployable individuals. The complainant then made annual access requests to EIC for information about the organization. He was well known to its staff and is alleged to have spoken openly about his requests for the centre's records.

When the latest request arrived, the manager simply assumed it was from the same person. As he said: "it didn't take a rocket-scientist to figure it out".

Without evidence to support the allegation that EIC revealed the source, the Commissioner concluded that the complaint was not well-founded.

Can mail blind persons' audio tapes "sealed"

A blind person complained that Canada Post's requirement that letter and talking book tapes be mailed unsealed violated his privacy rights.

The investigator found that blind persons can mail audio tapes free of charge. However, the material must be packaged so that Canada Post personnel can open it easily to ensure that it meets the regulations.

The complainant agreed to have the investigator discuss the matter with the Canadian National Institute for the Blind (CNIB). CNIB explained during the meeting that its free postage privilege amounts to an almost $3 million a year subsidy, which CNIB is reluctant to jeopardize.

Cassette tapes must be sent in special padded mailers. For talking books (the bulk of its mailings) CNIB has developed a re-usable plastic pouch with a Velcro closure. According to CNIB, this is as much for convenience as for ease of inspection. For other mailings, small padded envelopes are used and are either taped or stapled shut. Canada Post does not object to taping or stapling and the CNIB had never heard of a blind person being challenged on this type of closure.

CNIB pointed out that the regulations require that the closure permit easy inspection of the contents. It does not forbid sealing the envelopes. He suggested that the complainant simply staple his envelopes shut so that it would be relatively easy to tell if the envelope had been opened.

CNIB illustrated Canada Post's flexibility on the use of the free mailing privilege with anecdotes of blind individuals mailing back their cassette players to CNIB for repairs, claiming (and receiving) the free mailing privilege. According to CNIB, these mailings are definitely not covered by this privilege.

The investigator explained the entire procedure, as well as the CNIB's position, to the complainant. He was satisfied that Canada Post was not unnecessarily violating his privacy rights. The Commissioner concluded that the complaint was not well-founded.

Disclosure an error—but whose?

A complaint against the RCMP illustrated that sometimes it is impossible to get to the root a problem.

A man complained to the Commissioner when he learned that the RCMP had sent an unsolicited copy of his fingerprints and criminal records to Canada Post. There was no apparent reason for this disclosure since the man had received a pardon for his conviction. The records should have been sealed.

The investigator was unable to get a satisfactory explanation—audit trails were unclear and eventually the Privacy Commissioner's decision had to be based on "best available" information.

The investigation showed that in early 1991, Canada Post security received a copy of the complainant's criminal history record from the RCMP. Although this is normal procedure when its employees or candidates undergo security screening, security staff had no record of requesting the information. The complainant was not a employee, nor was he an applicant for a position. The record was put in a "pending" file.

At the investigator's request, the RCMP examined its records and found the distribution notation "Post Office, Ottawa" next to the man's criminal conviction listing. However, this did not explain why it had sent an apparently unsolicited copy of the record to Canada Post.

Further inquiries showed that the man had been briefly employed by Canada Post more than 10 years before. A reliability check (including fingerprinting) was done at that time. This explained the original distribution reference to the post office. Once he left the position, his personnel records—including his fingerprints—would normally have been transferred to the National Personnel Records Centre.

The complainant, once again a federal government employee, recently underwent a periodic review of his security clearance. This required the RCMP to process his criminal history record. Since no-one had removed the distribution notation on the old record, the updated record was sent to Canada Post.

This explanation is largely a reconstruction of events based on probabilities; it is not definitive. The Privacy Commissioner concluded that there had been an improper distribution of the information but, given the lack of detail, he could not say who was responsible.

However, he was able to reassure the man that Canada Post no longer possessed either the fingerprints or criminal history record and that the information had been well-protected for the brief period it was in Canada Post hands. The RCMP no longer has the fingerprints.

Denial "legal" but unnecessary

An Ottawa man asked the Commissioner to investigate his complaints against Consumer and Corporate Affairs (CCA), including one that alleged it had improperly denied him access to his personal information. He had lodged a complaint with CCA under the *Competition Act* and, unhappy with the investigation, wanted to see the comments about him in the file.

The Commissioner's investigation confirmed that CCA had withheld some information collected by its Director of Investigation and Research (DIR), claiming that it had been collected during a lawful investigation. Since the directorate is one of those units identified as "investigative bodies" in the *Privacy Act*, paragraph 22(1)(a) allows it to refuse to disclose information obtained in the course of its investigations.

The information requested was collected while DIR was investigating a complaint under the *Competition Act*. Thus it was lawful to refuse disclosure. However, the Commissioner observed that the exempted information was relatively innocuous and the complainant probably already knew its substance. Yet, representations and reasoning failed to persuade CCA to disclose the information. It clung steadfastly to its right to refuse, despite there being no reasonable probability that giving the man the information would harm the investigation or any person.

Since section 22(1)(a) does not require CCA to satisfy an injury test, the Privacy Commissioner had to tell the complainant that—much as he disagreed with CCA's stand—it complied with the letter of the law. He had to find the complaint not well-founded.

Ontario Workers' Compensation files no longer "confidential"

A lawyer complained that Health and Welfare Canada denied him access to 20 pages from his client's Canada Pension Plan disability medical file which had originated with the Ontario Workers' Compensation Board (WCB).

At Health and Welfare's suggestion, the lawyer applied directly to the WCB and received more material than Health and Welfare had exempted, leaving him unable to determine which documents Health and Welfare had used to deny his client's application. He argued that he could not properly represent his client in a pension appeal without knowing exactly which documents the department had received from the WCB.

The investigator found that Health and Welfare had withheld 20 pages using section 19(1)(c) of the *Privacy Act*. This section requires federal institutions to exempt information supplied "in confidence" by provincial governments or their institutions. There is no flexibility or discretion.

Thus, once a provincial or municipal government claims confidentiality, federal agencies may not disclose the information regardless of how innocuous it may be.

The investigation confirmed that a December 14, 1983, agreement provided that all information from the Ontario Workers' Compensation Board to Health and Welfare Canada was confidential and not to be disclosed except by the WCB itself.

Despite the agreement, the investigator persuaded Health and Welfare to ask WCB officials for permission to release the material. Health and Welfare did so and, as a result, WCB changed its policy, authorizing Health and Welfare to release its information directly to applicants. Health and Welfare then disclosed the client's material to the lawyer.

This is an important policy change which should simplify the procedure for many applicants.

The Commissioner concluded that the complaint was not well-founded because Health and Welfare previously had no authority to release the WCB's records. He applauded the change of position.

Notifying the Commissioner

Forty-three times this year the office was notified by government agencies that they intended to release personal information "in the public interest" or to "benefit" an individual. The Commissioner's role in this process is simply to notify the person if he considers it appropriate. He may advise against—but not prevent—the release.

Staff examine these notices so that the Commissioner remains free to consider any complaints without having prejudged the disclosure.

Although section 8(2)(m) of the Act is intended for exceptional disclosures, many notifications have become repetitive and something of an administrative burden for both the department and the Commissioner's office.

For example, Multiculturalism and Citizenship routinely notifies the Commissioner when confirming the Canadian citizenship of nominees for the Order of Canada. Since this was a recurrent and routine use of citizenship documents, the office suggested the department acknowledge this publicly and change its listing in *Info Source* to describe this use of citizenship documents. The department agreed, eliminating paperwork for itself and providing the public a clearer picture of how citizenship information may be used.

Correctional Services disclosures—a reprise

Last year the Commissioner reported on the difficult balance between individuals' privacy and the public interest—particularly on the release of reports on two prison escapes during which three persons were murdered (see Annual Report 1990-91).

The solicitor general refused to give the Justice and Solicitor General Committee uncensored versions of the investigation reports, maintaining that the *Privacy Act* prohibited the disclosure.

His refusal became the subject of a question of privilege in the House of Commons and the then-acting Privacy Commissioner was called to testify before the Privileges and Elections Committee. The acting Commissioner saw no difficulty with the solicitor general providing uncensored reports to an *in camera* committee hearing.

The privileges committee report concluded "that there is nothing in the *Privacy Act* to prevent the House of Commons from issuing an order for the production of unexpurgated versions of the two reports. Accordingly, we do not believe that an amendment to the *Privacy Act* to permit such production is either necessary or desirable".

The report suggested making copies available to the Justice committee at an *in camera* meeting.

The following are samples of other public interest notices received during the year.

Release prompts complaint to Commissioner

The Privy Council Office (PCO) advised the office that it intended to disclose personal information about several individuals to a professional body inquiring into the conduct of two of its members. The documents had been produced in evidence before a federal commission of inquiry.

PCO had obtained the consent of one individual (who was not under investigation) but considered it impractical to obtain everyone's consent. The Commissioner's office believed that the individuals should be notified of the impending release but suggested that it would be less disturbing coming directly from PCO. Privy Council agreed and wrote to each person, setting out the reasons for disclosure and citing the permissive section in the *Privacy Act*.

One of the professionals under investigation objected and has since complained to the Privacy Commissioner.

Details released for possible bravery award

The RCMP advised the Commissioner's office that the Chancellery of Canadian Orders and Decorations (in the Governor-General's Office) had asked the Force for information on one victim of a 1972 Arctic plane crash. The Chancellery was considering awarding a posthumous bravery decoration to a young Inuit man who survived the crash and kept the injured pilot alive but died before both could be rescued.

The Chancellery was reconsidering the award following publication of a second book on the accident which detailed the young man's role in the pilot's survival.

The privacy investigator examined the material that the RCMP proposed to release and found it contained less personal detail than the transcripts of a coroner's inquest or either book on the crash. The proposed disclosure did verify the accuracy of some of the details in the book.

The office did not object to the release and concluded it need not notify the sole survivor since the information was already public.

Pilots and engineers list not released

National Defence (DND) asked Transport Canada for a list of helicopter pilots and maintenance engineers in the Ottawa area to notify them of job opportunities at DND.

The Commissioner's office is reluctant to support this type of wide-scale list disclosure when there are other means of communicating with the individuals. Disclosure might "benefit" those who got jobs, but not the other several hundred who did not. The office suggested Transport Canada mail notices for DND, or that DND simply place advertisements in local newspapers and professional journals.

Transport Canada decided not to provide the list.

Post-mortem to family doctor

A doctor asked National Defence for the post-mortem of a military member who died suddenly while jogging. The doctor was treating a member of the man's family and wanted to determine whether the officer had the same condition which could contribute to a heart attack. Since the condition is suspected of being hereditary, the doctor wanted to begin immediate treatment of other family members.

DND released the post-mortem, then notified the Commissioner's Office. Although the Office prefers to be notified in advance, the request arrived during the public service strike when DND had no office staff. There was no objection to the disclosure.

Korean veterans' list to Rideau Hall

The Governor General's Office was the source of another request for personal information, this time about Korean War veterans. This notice provided a good example of how easily communications can become muddied over the telephone.

The Chancellery asked Veterans Affairs Canada for access to its computer database containing personal information about veterans eligible for the Canadian Volunteer Service Medal for Korea. The personal details—names and addresses, language, service number and confirmation of eligibility—would speed processing of applications for the new Korean War medal. The Governor General's office wanted to present the awards in November 1991.

Veterans Affairs staff telephoned the Commissioner's office to discuss the request and were left with the impression that they would need written consent from each veteran. (In fact, consent was just one of the avenues suggested.) This message was conveyed to Chancellery staff who, understandably frustrated, called the offices directly.

Privacy staff asked to see a written notification and sample of the information to be taken from the database. Once they had examined material, it was apparent that everyone on the list had indicated an interest in the medal and therefore would benefit. Staff also suggested Veterans Affairs obtain a written undertaking that the Chancellery would use the data only for this purpose, then destroy it or return it to Veterans Affairs.

The misunderstanding was cleared up quickly and the Governor General presented the first of the medals at a ceremony in Ottawa on November 10, 1991.

False claim to Canadian citizenship

External Affairs advised the Commissioner's Office that it proposed to tell a foreign government that a man arrested overseas on drug-related charges was not a Canadian citizen, even though he carried a Canadian passport.

The foreign government had seized the passport and given it to External Affairs on the understanding that if indeed he were Canadian, Canada would issue travel documents once the man was released. Since he was not a citizen, the Canadian embassy would not provide consular services or travel documents.

The Commissioner's Office agreed to the disclosure because there is a significant public interest in the integrity of Canadian passports. And it is important that Canadians not be alarmed by reports of consular services being denied to "citizens" whose claims are actually false.

Inquiries—the Public Talks Back

Inquiries officers continue to respond to an ever-mounting tide of letters and telephone calls—4,671 of them during the year. The offices' national toll-free line (shared with the Information Commissioner) is the only nation-wide access and privacy information service.

Canadians are becoming more aware of existing privacy protection, as well as new or proposed legislation governing provincial and municipal governments. Saskatchewan has just proclaimed its *Freedom of Information and Privacy Act*, and both British Columbia and Alberta have promised similar legislation in their latest throne speeches.

However, callers are shocked to discover that the private sector remains totally unregulated. The office handles many calls from individuals faced with difficulties in examining or protecting their information held by private organizations. It is frustrating to confess that there is nothing the office can do since our jurisdiction is limited to the federal government. Even worse is being unable to suggest a route to solve many callers' problems.

Although the *Privacy Act* is a federal law, hundreds of federally-regulated agencies and companies, and most Crown corporations, are "unregulated"—including Canadian National Railways, Via Rail, Air Canada, Atomic Energy of Canada Limited, various ports corporations, telephone companies and financial institutions such as banks and insurance companies.

The office has also answered calls about handling personal information in MPs' offices and at the Royal Commission on the New Reproductive Technologies. Employees and clients are dismayed to hear that we cannot intervene nor can they use provincial or municipal laws.

A substantial part of the inquiries officers' time is spent explaining the limited controls on use of Social Insurance Numbers (SIN). Most believe SIN use was restricted by the legislation which created unemployment and pension programs in the 1960s. Despite promises made at the time, that is not so. Many callers find it difficult to accept that only the federal government limits its use of SINs.

Individuals too often must choose between protecting their SIN or getting the goods and services they want. Given our limited mandate, staff now encourage callers to write to their MPs in the hope that if more MPs hear the complaints, they might act to control unnecessary uses of the SIN.

But the SIN story is not all gloom. Several organizations are interested in the SIN issue. During the past year, we sent background information to the Regional Municipality of Waterloo, the Ontario Ministry of Revenue, the Universities of Saskatchewan and Quebec, Nova Corporation and Maritime Telegraph and Telephone Company Ltd.

And there are kudos for the Quebec access and privacy commissioner's office for investigating SIN abuses in Quebec government agencies. Unlike most provinces which avoid the issue because SIN is a federal number, the Quebec commission seized the initiative and intervened under its own access and privacy legislation. For example, Quebec no longer demands a SIN to get a fishing permit for provincially controlled areas. As well, the automobile insurance industry has informally agreed to stop forcing clients to provide their SIN.

And the Quebec commission is now examining other provincial uses of the SIN including:

- Hydro-Québec's authority to use the SIN to identify both employees and subscribers;
- the Université de Laval's collection of SIN from students; and
- SIN use by hospitals, nursing homes and housing authorities.

It is encouraging to find that the federal government's efforts have had some impact outside its immediate jurisdiction.

Despite efforts to fine-tune listings in the blue (government) pages of telephone directories, more than half of the calls on the national toll-free line are unrelated to access or privacy. The receptionist re-directed 9343 callers to Reference Canada, the federal government's central information service. The office will make another attempt now that Bell Canada and the government telephone authority are working to improve the blue pages.

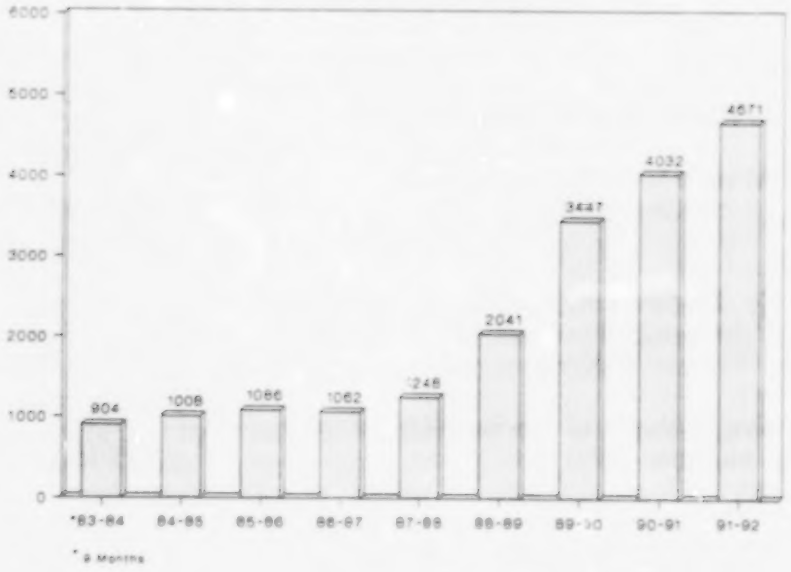
Finally, the office installed a device to communicate with callers with hearing or speech impediments (TDD).

The following two tables illustrate inquiries statistics. The first breaks out this year's inquiries by subject and the second compares numbers with previous years.

INQUIRIES 1991-92

What is the *Privacy Act* and How Can I Use It?	2420 (52%)
No Jurisdiction/Outside *Privacy Act* (Federal, Provincial, Municipal & Private Sectors)	808 (17%)
Use & Abuse of the Social Insurance Number (SIN)	588 (13%)
Misdirected Applications & Unrelated Matters	855 (18%)
TOTAL	4671

Inquiries 1983-92



Compliance Directorate

The directorate had two objectives for 1991-92. The first was to focus on a complex national organization—Canada Mortgage and Housing—with significant electronic data processing and communications components. Auditing CMHC permitted staff to examine distributed data processing and electronic communication issues and to further develop our EDP audit methodology.

The second objective was to review several smaller agencies dealing with women's and minority rights. Most of these organizations have large personal information collections, often because they investigate complaints. We selected Status of Women Canada, Canadian Advisory Council on the Status of Women, the Canadian Human Rights Commission and the Immigration and Refugee Board.

Audits were also completed on several other institutions such as National Defence, the National Capital Commission, Canadian Film Development Corporation, the Standards Council of Canada and various pilotage authorities. Work at 13 other organizations will carry over to 1992-93. Staff also

- investigated five incidents of lost or stolen files;
- audited three existing data-matches at Employment and Immigration Canada; and
- conducted a government-wide survey on the use of upward or reverse appraisals in federal institutions.

Trends and Problems

The past year's audits revealed some emerging trends in government information handling that demand attention. Foremost perhaps is the federal government's increasing use of private sector companies to provide services which handle personal information.

Contracting out—who's minding the data?

Budget pressures on government agencies have led many to use private industry for some of the services once performed in-house. For example, services such as Employee Assistance Programs, payroll applications and credit checking—and the personal information that goes with them—are now frequently handled by private companies under contract to the responsable government agencies.

The office has no quarrel with private companies performing services. However, unlike the federal government, the private sector is not covered by the *Privacy Act*. Thus, personal files handed over to private firms get no formal privacy protection unless specific clauses are written into the contracts. Since some departments use standard Supply and Services Canada contract forms and others draft their own, there is little consistency. Nevertheless, almost without exception, the contracts are deficient.

For example, contracts fail to:

- define ownership of the information;
- ensure employee access to the files;
- restrict further use of the personal data;
- protect against unauthorized disclosure;
- ensure proper disposal of files at contract end;
- establish retention and disposal criteria; and
- ensure the department's ability to audit compliance.

Our office is now working with Supply and Services Canada and Treasury Board to develop a standard contract. This should remedy many of the problems.

Checking employee credit ratings

Compliance auditors have found collection problems during examinations of personnel files. All permanent government employees—and many of those transferred or promoted—must undergo reliability checks. The department or agency obtains candidates' permission to check their credit ratings. Ratings are a combination of letters and numbers which describe the person's relative debt load and repayment behaviour.

The staff also found many of the same contracting problems described earlier. However, the credit checking process revealed other potential problems. For example, such large organizations as the RCMP, Canada Mortgage and Housing and National Defence often have direct on-line access to credit bureaus, allowing them to obtain substantially more personal financial data than a simple credit rating. There appears to be potential for abuse and nothing to prevent institutions from going on fishing expeditions.

In fact, most audited institutions tended to collect much more financial information than they needed. Details such as credit limits and account balances were found in files where only a simple credit rating was required. As well, the staff found credit reports containing not only the employee's information but also data on spouses. Credit bureaus often send out a work history and credit rating on the spouse, linking the information with the employee by Social Insurance Numbers and dates of birth.

Once in the hands of the government agency, credit information is often not kept secure. In some instances privacy staff found the information was transmitted by fax. In others, it was stored on the hard disk of desktop computers without adequate security protection.

Finally, much credit information is unreliable and therefore government institutions may be relying on incorrect data. Independent studies reveal a high error rate in credit files. Updates and corrections are made slowly and—sometimes—not at all. The onus rests entirely with individuals, even though stores and banks transmit the information to the credit bureaus.

Electronic transmission of personal information

Privacy audits have also found that government institutions routinely fax personal information. This courts the risks of having the transmission intercepted or sent to the wrong location. For example, an employee at the Canada Employment Centre in Sarnia, Ontario, sent four individuals' unemployment insurance queries to the local newspaper instead of the Employment and Immigration Canada office in London, Ontario. The employee had mistakenly punched the adjacent speed dial button which was programmed with the newspaper's number.

The incident was simple human error but it demonstrated the possible consequences of faxing personal information—a procedure auditors found in almost every institution visited. Fax is one type of technology where policies and procedures are not keeping pace. Little thought is given to what information should or should not be sent by fax. Employees transmit personal information from the most innocuous (lists of participants at meetings) to the most sensitive (medical records and credit checks).

Similar difficulties arise with the new electronic mail (E-mail) systems now being widely implemented. E-mail programs allow users of computer networks to communicate and transfer data within the network. Yet there are few policies or procedures to ensure that the data are shared only with those who need to know, or that it all remains secure.

Who's minding the computer?

One disturbing trend is that government seems not to be applying the same standards of management and control to its EDP resources as it does its paper records. Large complex government institutions appear not to know what hardware and software they own, let alone who has access and how the systems are being used. Increasingly, major collections of personal records are being automated but without formal controls. Electronic files lend themselves easily to improper collection, use and disclosure but, because the data are out of sight, they appear to be out of mind.

Portable computers: Automation of the federal government has seen the computer shrink from yesterday's roomful of equipment to today's notebook-sized units (with as much or more power) tucked into a briefcase. And already being tested is integrated chip technology which makes the plastic card "smart"—a mini-computer capable of storing and processing information.

However, these personal computing devices demand new management and control systems. Users often forget that these are not merely miniature typewriters. Computers remember what they process. Their loss or theft means not only lost valuable equipment but also lost information.

The office investigation this year of the theft of a personal computer from the Montreal office of Veterans Affairs illustrates the seriousness of such an incident. The computer was part of a new system on trial. It had been loaded with tombstone data on the office's entire 20,000 client base. Fortunately the personal details were very limited and the Commissioner decided not to notify the individuals concerned.

The investigation made it clear that Veterans Affairs staff had not followed the department's procedures for protecting valuable property. More important, however, investigators found no policies and procedures covering the storage and protection of the personal data in the computer memory. The Commissioner recommended that Veterans Affairs develop those policies and consider restricting storage of personal data to diskettes which could be removed and stored separately. Alternatively, personal data on personal computers could be encrypted to make it inaccessible to unauthorized users.

Controlling access in networks: The marriage of microcomputers and local or wide area networks poses another privacy challenge: determining which users should have access to what data. Auditors often find that authorized system users frequently can access information they do not need. The physical premises and the computer system may be secure from external threats but, once into the system, authorized users may access any data. Systems are needed to restrict users to the information they need to know.

Ending the pack rat syndrome: Auditors find few retention and disposal schedules for EDP files and those that do exist often do not correspond to the schedules for the paper files. Government may be shredding its paper but much of that paper was generated electronically. The data are replicated on hard and soft disks that seem to be kept indefinitely. Government agencies managing the retention and disposal of personal files need also to examine the electronic versions.

Describing information holdings

The description of government information holdings in *Info Source* continues to concern the Commissioner. Lack of resources may be a contributing factor but auditors find that *Info Source* is an incomplete and sometimes inaccurate catalogue of personal information held by government institutions. Some departments seem not to have a clear understanding of what they should list or how to change listings.

A common problem is the failure to list such federal employee standard banks as leave and attendance, travel and relocation, and training and development. The reverse is sometimes true—standard banks are listed but the institution holds no information. In fact, the bank is empty. And occasionally auditors and complaints investigators stumble upon information that seems not to be listed at all.

It may be time for Treasury Board to set out more clearly what institutions should describe and how to make changes. Also needed is a more rigorous review of the input government institutions provide to *Info Source*.

Upward appraisals

In earlier reports, the Privacy Commissioner expressed concern about the anonymity feature of upward or reverse appraisal processes being conducted in some departments. This process allows employees to rate and comment on their manager's performance, often anonymously.

In an effort to establish just how widespread the upward appraisal process has become and how it is being done, the Compliance Directorate polled 148 departments and agencies covered by the *Privacy Act*. At this writing it had received 141 responses (eight from one department), 27 of which were using or planning to use the process within the next 12 months. Of these 27, 24 promise employees anonymity and 18 use private consultants to analyze the results.

So fewer than 20 per cent of government agencies have embraced the idea. Nevertheless, one questions Canada's public service lending itself to a personnel relations process which relies upon the use of anonymous informants.

Corporate Management Branch

Corporate Management provides both the Privacy and Information Commissioners' offices with financial, administrative, informatics and library services.

The following are the offices' expenditures for the period April 1, 1991, to March 31, 1992. *

	Information	Privacy	Corporate Management	Total
Salaries	1,670,069	1,911,442	658,825	4,240,336
Employee Benefit Plan Contributions	285,600	307,020	121,380	714,000
Transportation and Communication	75,621	59,500	124,875	259,996
Information	21,005	55,261	3,109	79,375
Professional and Special Services	209,028	190,237	81,059	480,324
Rentals	4,391	3,276	11,945	19,612
Purchased Repair and Maintenance	6,688	6,358	7,199	20,245
Utilities, Materials and Supplies	18,692	9,814	29,070	57,576
Acquisition of Machinery and Equipment	109,474	44,361	12,959	166,794
Other Payments	2,970	1,873	250	5,093
TOTAL	2,403,538	2,589,142	1,050,671	6,043,351

* Expenditure figures do not incorporate final year-end adjustments reflected in the offices' 1991-92 Public Accounts.

Finance

The offices' total resources for the 1991-92 fiscal year were $6,691,000 and 82 person-years, an increase of $367,000 and four person-years over 1990-91. Personnel costs of $4,954,336 and professional and special services expenditures of $480,324 accounted for more than 90 per cent of expenditures. The remaining $608,691 covered all other expenses.

Personnel

In the spirit of PS 2000, the unit made several improvements to the offices' personnel management practices by recruiting a management trainee, developing incentive awards and an orientation program for new employees, and streamlining some of its personnel procedures. In addition, the unit conducted a triennial classification audit, followed up the 1987 official languages audit and signed a letter of understanding on official languages with the Treasury Board.

Administration

The unit made continued progress on a retention and disposal schedule for records and also on an automated inventory of assets. As well, it evaluated the offices' telephone system to improve service to the public.

Informatics

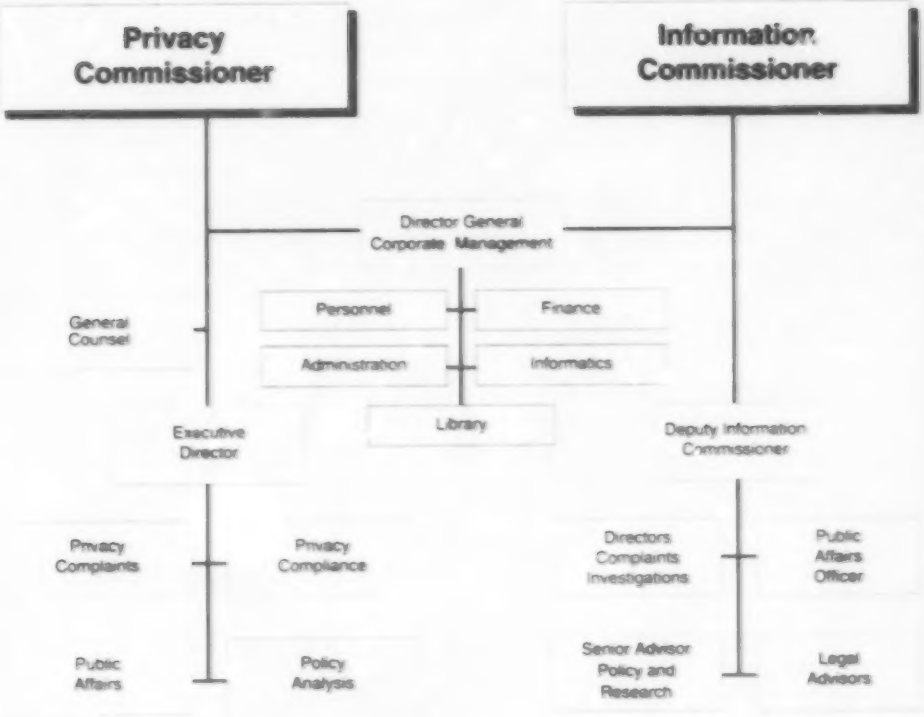
This year the unit completed three studies for a new case management system, office automation and using a computer network in a secure environment.

Library

The library provides interlibrary loan services, manual and automated reference and research, and subject-oriented media monitoring files. In addition to acquiring information on freedom of information, the right to privacy, data protection and the ombudsman function, the library has a special collection of Canadian and international ombudsmen's reports and departmental annual reports on the administration of the two acts.

The library (which is open to the public) handled 1,298 publication requests and answered 1,084 reference questions during the year.

Organization Chart



Rapport annuel du Commissaire à la protection de la vie privée 1991-1992

Page couverture: Les nouvelles "cartes à mémoire" ressemblent à des cartes bancaires ou à des cartes de crédit mais avec une différence importante. Un microprocesseur enchâssé permet le traitement et l'emmagasinage de l'information en plus d'en identifier le propriétaire. Les symboles qui suivent illustrent l'éventail de services et de renseignements personnels qu'on pourrait bientôt retrouver sur un seul petit morceau de plastique. Ceux-ci sont:

- Carte d'appel téléphonique
- Laissez-passer
- Prestations fédérales
- Services bancaires
- Achats au détail
- Dossiers médicaux
- Accès au système informatique
- Accès au domicile et au travail

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent,
Ottawa (Ontario)
K1A 1H3

(613) 995-2410, 1-800-267-0441
Télec. (613) 995-1501
ATS (613) 992-9190

© Ministre des Approvisionnements et Services Canada 1992

N° de cat. IP30-1/1992

ISBN 0-662-59183-6

L'honorable Guy Charbonneau
Président
Sénat
Ottawa

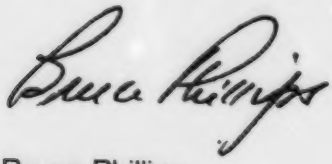
le 12 août 1992

Monsieur Charbonneau,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1991 au 31 mars 1992.

Veuillez agréer l'expression de mes sentiments respectueux.

Le Commissaire à la protection de la vie privée



Bruce Phillips

L'honorable John A. Fraser, c.p., c.r., député
Président
Chambre des communes
Ottawa

le 12 août 1992

Monsieur Fraser,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1991 au 31 mars 1992.

Veuillez agréer l'expression de mes sentiments respectueux.

Le Commissaire à la protection de la vie privée

Bruce Phillips

Table des matières

Mandat 1

Le début de la fin? 3
La protection de la vie privée par la Charte 10
La protection de la vie privée dans les secteurs des banques et des télécommunications 12
Le secteur privé : une réglementation volontaire 14
La protection de la vie privée au travail 17
Une loi perfectible 18
Une nouvelle définition des "renseignements personnels" 20
Resserrement des conditions sur la comunication des renseignements personnels 21
Élargissement du critère du préjudice causé aux personnes concernées 24
L'absurde érigé en système 27

Le dépistage génétique 29

Une année dans les tranchées de la vie privée 34
Les appareils de télécommunication : c'est jouer avec la vie privée 34
Et la saga du NAS continue 40
Derniers progrès technologiques 44
Couplage de données 49

La division des plaintes 53
Quelques cas 66
Aviser le Commissaire 83
Demandes de renseignements - Le public réagit 90

Direction de l'observation 97
Tendances et problèmes 98
Contrats accordés à l'extérieur – Qui surveille? 98
Vérification de la cote de crédit des employés 100
Transmission électronique de renseignements personnels 102
Qui surveille l'ordinateur? 104
Évaluations vers le haut 108

La gestion intégrée 109

Organigramme 112

Mandat

La *Loi sur la protection des renseignements personnels* donne aux individus accès à leurs renseignements personnels détenus par le gouvernement fédéral; protège la vie privée des individus en restreignant le nombre des personnes qui peuvent consulter les renseignements; et donne aux individus un certain contrôle sur la collecte et l'usage des renseignements par le gouvernement.

La Loi énonce les principes des pratiques équitables en matière d'information qui exigent que le gouvernement:

- ne collecte que les renseignements dont il a besoin pour exécuter ses programmes;
- recueille les renseignements directement auprès de l'individu concerné, dans la mesure du possible;
- informe l'individu des fins auxquelles ils sont destinés;
- conserve les renseignements suffisamment longtemps pour en assurer l'accès aux individus; et
- veille « dans la mesure du possible » à ce que les renseignements personnels soient exacts et complets.

Toute personne présente au Canada peut déposer une plainte auprès du Commissaire à la protection de la vie privée si:

- elle s'est vu refuser une partie quelconque des renseignements;
- le droit de demander la correction de certains des renseignements contenus dans le fichier ou de les annoter leur est refusé;
- le ministère prend plus des 30 jours initiaux ou des 60 jours maximums pour fournir les renseignements;
- la description du contenu des fichiers de

renseignements donnée dans le manuel *Info Source* est incorrecte à un quelconque égard;

- la liste donnée dans ce manuel pour chaque ministère ne décrit pas tous les usages qui sont faits des renseignements personnels;
- une institution recueille, conserve, utilise ou élimine des renseignements personnels d'une manière qui contrevient à la *Loi sur la protection des renseignements personnels*.

Les enquêteurs du Commissariat à la protection de la vie privée examinent tous les fichiers (y compris ceux considérés inconsultables), à l'exception des renseignements confidentiels du Conseil privé de la Reine, pour s'assurer que les institutions fédérales se conforment à la Loi.

La Loi confère également au Commissaire à la protection de la vie privée le pouvoir de vérifier la façon dont les institutions fédérales recueillent, utilisent et disposent des renseignements personnels, sans devoir attendre qu'une plainte soit déposée.

La fin du début?

C'est peut-être trop tenter la fortune, mais l'auteur de ces lignes est quand même prêt à mettre sa boule de cristal - et sa réputation - en jeu pour oser dire que le dossier de la protection de la vie privée semble s'améliorer un peu.

Bien sûr, nous sommes encore loin du beau fixe! Les zones sinistrées abondent toujours et les vestiges de nombreuses défaites jonchent le terrain.

Néanmoins, pour paraphraser outrancièrement Churchill, même si nous sommes loin du début de la fin des problèmes, nous sommes peut-être près de la fin du début.

Bref, disons-le clairement, il semble y avoir eu des progrès.

Au cours de l'année à l'étude, un certain nombre d'événements survenus dans plusieurs secteurs laissent entendre que les forces de la protection de la vie privée - si lentes à se mobiliser - commencent à se faire sentir.

Tant au gouvernement que dans le secteur privé, il y a des signes encourageants d'une sensibilisation accrue aux problèmes de protection de la vie privée, et les gens semblent plus disposés à y chercher remède. Voici quelques-uns des exemples les plus frappants de cette évolution.

• Deux nouvelles provinces, la Colombie-Britannique et la Saskatchewan, sont à se doter d'organismes de protection de la vie privée et une troisième, l'Alberta, envisage de leur emboîter le pas. Quand elles auront toutes trois fait le nécessaire, il y aura des mécanismes de protection des renseignements personnels et de la vie privée dans toutes les provinces du Canada, du Québec à la côte du Pacifique.

• L'activité législative fédérale dans les secteurs des télécommunications et des institutions financières a focalisé intensément l'attention sur les aspects de protection de la vie privée de ces deux secteurs, aussi bien dans l'administration fédérale qu'au Parlement. Certaines des réactions envisagées - à l'étude au moment d'aller sous presse - pourraient permettre une percée dans ce dossier difficile, en assurant une protection accrue de notre intimité dans le secteur privé.

• Certains des principaux intervenants réagissent maintenant de façon plus énergique à la sensibilisation croissante d'un public mécontent de la façon dont le monde des affaires traite les renseignements personnels qu'il détient. À cet égard, les entreprises canadiennes de marketing direct méritent une mention honorable. En effet, s'il est adopté, le code dont elles envisagent de se doter nous donnera au moins l'espoir que ceux d'entre nous qui ne veulent pas recevoir de courrier indésirable ni être sollicités au téléphone par des vendeurs auront un moyen pratique - annoncé à grand renfort de publicité - d'y échapper.

• Quoique techniquement cela n'ait pas eu lieu cette année, le Conseil canadien de la radiotélévision et des télécommunications a rendu une décision qui fera époque, dans le dossier de «l'Afficheur», en établissant le principe critique que les abonnés qui veulent préserver la confidentialité de leur numéro de téléphone ne devraient pas avoir à payer un supplément à cette fin. Cette décision capitale reconnaît clairement que, dans le domaine des télécommunications, la protection de la vie privée est un droit acquis du consommateur plutôt qu'un simple «produit» à vendre.

Nous reviendrons plus longuement sur certains de ces points dans les pages suivantes. La liste qui précède n'est pas un relevé exhaustif de ce qui s'est produit dans les nombreux secteurs de la vie et du commerce qui ont eu cette année un impact sur la protection de la vie privée; elle ne contient que des exemples d'une tendance encourageante! Néanmoins, pris individuellement ou collectivement, s'ils sont bien moins que des victoires éclatantes, ces exemples sont certainement bien préférables au statu quo.

Cependant, il reste que tout cela doit être interprété dans un contexte d'une autre envergure. Le fait est que toutes les pressions des partisans de la protection de la vie privée n'ont jusqu'à présent pas eu d'effet sur le problème le plus crucial et le plus fondamental de la protection de la vie privée, à savoir l'énorme trafic des renseignements personnels qui échappe à toute réglementation et dont le chiffre d'affaires - en

Amérique du Nord seulement - représente des milliards de dollars. Une société qui accepte sans sourciller que des inconnus possèdent des dossiers à l'exactitude incertaine sur des millions de personnes et ce sans droit d'accès et de correction, c'est une société téméraire par son indifférence à la préservation de l'aspect le plus fondamental de la protection de la vie privée : le droit des gens à un certain contrôle sur ce que les autres savent à leur sujet. Et pourtant, telle est la situation d'aujourd'hui. Nous sommes à peu près tous fichés dans au moins un - et probablement bien plus d'un - des fichiers informatiques des banques de données et autres marchands de listes.

Il s'agit toutefois d'indifférence largement imputable à l'ignorance. De nombreuses preuves manifestes démontrent que, chaque fois que le public comprend clairement la situation et qu'il a la possibilité d'intervenir, des légions de partisans de la protection de la vie privée montent sur les barricades, parfois avec des résultats étonnants.

Par exemple, il y a quelques années, une compagnie de téléphone américaine avait demandé à ses abonnés s'ils s'opposeraient à ce que les renseignements personnels qu'elle détenait sur eux soient vendus à d'autres entreprises. Quand 800 000 abonnés ont dit qu'ils s'y opposeraient, la compagnie a laissé tomber. Et le jour où l'une des grandes entreprises de production de listes des États-Unis a avancé l'idée de commercialiser un disque lisible par machine contenant des renseignements sur 80 millions de personnes, l'idée a provoqué une telle controverse qu'elle a été abandonnée, elle aussi.

La réaction du public à l'explosion du marketing direct est un autre indice de l'importance critique d'une meilleure sensibilisation du public à ces questions. Nous ne prétendons pas que les entreprises de marketing direct sont dépourvues du sens des responsabilités, mais il faudrait être naïf pour ne pas reconnaître que c'est l'inquiétude du public quant aux moyens utilisés par ces compagnies pour obtenir leurs renseignements qui les a incitées à se doter d'un meilleur code de protection de la vie privée.

Par conséquent une meilleure compréhension des problèmes de protection de la vie privée par le public, dans le contexte de la technologie moderne, est une absolue nécessité. Existe-t-il un exemple plus simple et plus percutant que l'expérience vécue récemment avec les téléphones cellulaires?

À la lecture de notre dernier rapport annuel, bien des gens semblent avoir été étonnés d'apprendre que les conversations par téléphone cellulaire pouvaient facilement être interceptées avec du matériel facile d'accès. Cette révélation n'a pas réduit l'engouement du public pour des appareils aussi utiles, mais je parierais que bien des gens sont désormais beaucoup plus prudents lorsqu'ils les utilisent.

En fin de compte, dans le dossier du téléphone cellulaire, la seule donnée manquante était de l'information. La couverture que les médias ont accordée à nos observations a largement contribué à y remédier, mais il n'y aurait pas eu de lacune si les compagnies avaient eu l'obligation de veiller à ce que leur clientèle obtienne toute l'information nécessaire pour prendre des décisions judicieuses sur ces appareils.

L'obligation d'informer les gens vaut autant pour le secteur privé que pour le secteur public. Dans ce secteur, le seul organisme national qui cherche à suivre constamment l'évolution du dossier global de la protection de la vie privée est précisément le Commissariat à la protection de la vie privée, qui est par conséquent le mieux placé pour jouer un rôle de leader dans l'éducation du public et dans les communications à ce sujet. Et pourtant, le Commissariat n'a pas mandat de faire l'éducation du public, bien que même des parlementaires soient étonnés de se le faire dire. Nous faisons ce que nous pouvons avec des ressources quasi inexistantes, grâce essentiellement au rapport annuel, à des discours et à des conférences, quand le temps nous le permet, et grâce aussi aux bons soins des médias, reconnaissons-le.

Aucun de ces facteurs ne doit être négligé, et surtout pas le dernier. Néanmoins, il est possible et souhaitable de faire beaucoup plus. On a peut-être oublié que le gouvernement s'était engagé en 1987 à réviser la *Loi sur la protection des renseignements personnels* afin de doter le Commissariat d'un mandat visant l'éducation. Souhaitons que ce rappel fera progresser le dossier.

Au fil des années, le Commissaire et son prédécesseur ont discouru sur l'opportunité d'étendre la portée de la *Loi sur la protection des renseignements personnels* aux organismes privés de compétence fédérale, comme

les banques et les entreprises de transport. Pour sa part, le Commissaire actuel a toujours cru que ce n'était pas la meilleure, mais peut-être la seule chose à faire, étant donné l'impossibilité manifeste d'assurer autrement une protection efficace de la vie privée dans le secteur privé. L'urgence du problème s'atténue dans une certaine mesure, étant donné que le Parlement étudie les incidences sur la protection de la vie privée des projets de loi que le gouvernement a déposés à l'égard des institutions financières et des télécommunications. Il faudra en attendre les résultats pour savoir si cette approche ponctuelle est la meilleure. C'est d'ailleurs l'approche que les Pays-Bas sont en train d'adopter. Par exemple, dans le cas des banques canadiennes, l'Association des banquiers canadiens elle-même, et plusieurs de ses membres se sont déjà donné des codes de protection de la vie privée qui, une fois améliorés, pourraient fort bien devenir le noyau d'un ensemble de règlements sur la façon des banques de traiter les renseignements personnels. Le principal élément manquant dans les codes actuels est un système indépendant de supervision et de règlement des différends, indispensable pour assurer le respect des règlements et la confiance du public. Quoi qu'il en soit, il est plus urgent de sensibiliser davantage les citoyens et de mieux les informer, car un public bien informé est la meilleure défense contre les abus. C'est aussi vrai pour la protection de la vie privée que pour celle de la démocratie dans son ensemble, et c'est certainement un élément indispensable à toute défense efficace.

La protection de la vie privée par la Charte

L'importance d'un public bien informé doit en outre être envisagée dans le contexte d'une nation dont la Constitution ne reconnaît toujours pas clairement le droit à l'intimité. Même s'il existe diverses lois comme au fédéral la *Loi sur la protection des renseignements personnels*, qui accordent aux citoyens une certaine protection dans des domaines bien précis de la collecte de renseignements, et même si la Cour suprême a reconnu un droit à l'intimité dans certains arrêts portant essentiellement sur des questions de droit pénal, il n'en demeure pas moins que l'acceptation du droit à l'intimité comme droit fondamental de la personne n'a toujours pas été entériné dans les lois du pays.

Le Commissariat a tenté d'y remédier, en présentant au Comité spécial mixte sur le renouvellement de la Constitution du Canada une communication dans laquelle il l'a pressé d'inclure le droit à la protection de la vie privée dans ses recommandations.

Dans ce document, le Commissaire a souligné que le droit à l'intimité figurait dans ce qui était presque la toute première ébauche de la *Charte des droits et libertés* et qu'il fait déjà partie intégrante de plusieurs documents analogues, tels que la *Charte des droits de Québec*, la *Déclaration universelle des droits de la personne*, la *Convention européenne sur les droits de la personne* et les constitutions de plusieurs états des États-Unis d'Amérique, pour ne citer que quelques-uns de ces documents. De plus, l'idée a été favorablement accueillie par le Comité de la justice de la Chambre des communes (en 1987) et elle a été appuyée par des organismes nationaux importants, comme l'Association du barreau canadien.

Malheureusement, la proposition du Commissariat n'a pas été appuyée par la majorité des membres du Comité. Bien entendu, nous ne savons pas exactement de quoi le Comité a discuté à *huit clos*, mais nous avons cru comprendre que certains de ses membres ont dit craindre que l'inclusion d'un droit à l'intimité dans la Constitution risquerait de limiter d'autres droits ou libertés (comme la liberté d'expression ou le droit d'accès à l'information). À cet égard, on devrait souligner qu'un éventuel droit à l'intimité ne devrait être accordé qu'à condition que l'intérêt privé et l'intérêt public soient conciliés, comme pour tous les autres droits et libertés déjà garantis par la *Charte*. En effet, la *Charte* précise que ces droits doivent être exercés de façon raisonnable dans une société libre et démocratique, ce qui impose aux tribunaux le devoir de concilier les prétentions contradictoires ou conflictuelles.

Le sort réservé à cette initiative a été d'autant plus décevant que l'épuisement général qui suivra vraisemblablement la fin de la ronde actuelle de négociations constitutionnelles risque fort d'empêcher pour longtemps toute tentative de modification de la *Charte*. Cela dit, la question reste entière pour le Commissaire, et le Commissariat continuera à faire valoir son point de vue.

La protection de la vie privée dans les secteurs des banques et des télécommunications

Au palier fédéral, nous avons peut-être franchi un point de non-retour depuis que figurent dans deux importants projets de loi des dispositions susceptibles de répondre aux préoccupations des partisans de la protection de la vie privée. Le premier de ces projets de loi est la nouvelle version de la *Loi sur les banques* et des textes légaux qui en découlent; il sera désormais possible pour des institutions financières comme les banques d'être propriétaires de compagnies d'assurance et de fiducie, et vice versa. Or, les institutions financières disposent d'une telle masse de renseignements personnels que le Commissariat s'inquiète tout naturellement de la mesure dans laquelle elles pourraient partager ces renseignements, ainsi que du degré de consentement et de contrôle des clients et des consommateurs sur ce genre d'échange d'information.

Le projet de loi donne aux autorités gouvernementales le pouvoir d'adopter des règlements à ce sujet. En avril, le Commissaire a comparu devant le Comité sénatorial des banques pour inviter instamment le Parlement à se prévaloir de ce pouvoir d'adopter des règlements.

Le Comité a manifesté beaucoup d'intérêt pour cette recommandation et déclaré que le Commissaire pourrait être invité à lui en reparler. Le Commissaire d'ailleurs sait que le ministère des Finances se penche lui aussi sur la question.

Cela dit, le nouveau projet de loi sur les télécommunications que le Parlement étudie présentement est encore plus explicite : il reconnaît que la protection de la vie privée est l'un de ses objectifs. Hormis la *Loi sur la protection des renseignements personnels*, c'est selon le Commissaire, la première loi connue à contenir une disposition aussi explicite.

Au moment d'aller sous presse, le résultat de ces initiatives n'est pas encore connu. Cependant, le Commissaire se dit content de voir cette preuve d'une compréhension croissante des problèmes de protection de la vie privée aussi bien chez les législateurs que dans l'administration fédérale.

En fait, le Commissaire estime qu'on peut voir là une possibilité de solution - ou à tout le moins l'ébauche d'une solution - au problème si souvent débattu de la régulation des pratiques de traitement des renseignements personnels du secteur privé. Toujours dans le domaine législatif, le Commissaire remarque avec beaucoup de satisfaction la proclamation de la *Loi de la Saskatchewan sur l'accès à l'information et sur la protection des renseignements personnels*, ainsi que de l'intention du gouvernement de la Colombie-Britannique de déposer sous peu un projet de loi analogue. À cette fin, la Colombie-Britannique a retenu les services du professeur F. Murray Rankin comme principal expert-conseil, ce qui l'assure que sa démarche bénéficiera d'un dévouement exceptionnel et de connaissances très étendues.

L'introduction d'une protection de la vie privée dans la troisième province la plus peuplée du Canada signifie que plus de 60 pourcent des Canadiens bénéficieront bientôt d'un service provincial de défense de leur intimité, (les Québécois et les Ontariens en ayant déjà un). Le Commissaire est heureux de pouvoir dire qu'il a eu des discussions avec les autorités d'une autre province où l'on envisage aussi l'adoption d'une loi analogue.

Tous ces faits nouveaux sont très positifs, car ils prouvent bien que nos élus reconnaissent de plus en plus la protection de la vie privée non seulement comme un droit pour chacun de nous, mais aussi comme un droit qu'il faut étayer par des lois et des règlements pour le défendre contre une technologie de plus en plus intrusive.

Le secteur privé : une réglementation volontaire

Comme nous l'avons mentionné auparavant, une grande partie du secteur bancaire canadien est désormais volontairement régie par des codes de protection de la vie privée. L'Association des banquiers canadiens a amorcé cette démarche en promulguant un modèle de code, et plusieurs des plus importantes banques à charte en ont adopté un par la suite. Les détails de ces codes diffèrent, et aucun n'est idéal, mais ils se ressemblent tous sur un point important : ils reconnaissent que le sort réservé aux renseignements personnels que les clients et consommateurs divulgent aux banques les intéresse, et qu'ils ont le droit à la fois de consentir à ce que les institutions bancaires s'en servent et de contrôler cet usage.

Au moment d'aller sous presse, et pour des raisons que nous avons déjà mentionnées, ces mesures encourageantes bien qu'imparfaites pourraient avoir été supplantées par un règlement adopté en vertu de la nouvelle *Loi sur les banques*. Si c'était le cas, cela serait l'amorce d'une importante collaboration entre les autorités gouvernementales et celles du secteur privé. D'un autre côté, si ce n'était pas le cas, le Commissaire demeure convaincu que, bien qu'il faille féliciter les banques pour les progrès qu'elles ont réalisés jusqu'à présent, leurs codes manquent toujours de vigueur.

Nous nous devons aussi de répéter qu'il y a des signes de progrès encourageants dans le secteur du marketing direct, qui a fait l'objet ces dernières années de bien des préoccupations et de nombreuses plaintes du public. Le Commissaire a déjà applaudi la décision de l'Association canadienne du marketing direct (ACMD) de créer un système grâce auquel les Canadiens pourraient faire rayer leurs noms des listes que détiennent les compagnies qui en sont membres. Depuis, l'ACMD a continué à élaborer un code élargi. Ce code n'est pas encore publié, mais le Commissaire espère ardemment qu'il donnera aux consommateurs un rôle beaucoup plus important à jouer, au moins dans la mesure où il sera interdit d'inscrire leur nom sur des listes de ce genre sans leur consentement.

Signalons aussi une autre initiative prometteuse prise au cours de l'année, celle-là par l'Association canadienne de normalisation (ACNOR), qui a pour principale responsabilité d'assurer la sécurité et la fiabilité des produits mis en marché au Canada. Son logo (CSA), qu'on retrouve sur les produits conformes aux normes de l'entreprise privée, est bien connu des Canadiens.

Peu de temps après que le Commissaire eut parlé du projet de directive européenne sur la protection des données personnelles dans son dernier rapport annuel, l'ACNOR a communiqué avec le Commissariat pour lui faire la proposition suivante : mettre sur pied un comité chargé d'élaborer un code modèle de protection des renseignements personnels, code qui pourrait servir de norme nationale minimale pour les organismes du secteur privé qui traitent des renseignements personnels.

L'ACNOR est l'organisme idéal pour développer un tel code. Organisme de service indépendant, il est composé de représentants des gens d'affaires, de l'industrie privée, des syndicats, des universités et des organismes de réglementation. La proposition de l'ACNOR est un prolongement naturel de ses activités de normalisation de la technologie internationale et de son intérêt pour l'impact de la technologie sur les consommateurs, les entreprises et l'industrie privée.

L'adoption d'un code modèle de pratique pour le secteur privé nous donnerait un moyen de concilier les intérêts commerciaux et le droit inhérent des consommateurs à l'intimité. Par ailleurs, l'établissement d'un code confirmerait l'engagement des entreprises canadiennes à respecter les principes de protection de la vie privée énoncés dans les lignes directrices de l'OCDE, et donc de satisfaire à la condition posée par la Communauté européenne qui exige une protection équivalente ou adéquate.

Le comité d'établissement du code de l'ACNOR (sur lequel le Commissariat est représenté) a rédigé une proposition qui lui a déjà valu des déclarations d'intérêt et des subventions d'AMEX, de Readers' Digest, de Bell Canada, d'Equifax et des ministères fédéraux Consommation et Affaires commerciales Canada ainsi que des Communications.

Au besoin, l'ACNOR embauchera un expert-conseil d'expérience qui fera des recherches et poursuivra l'élaboration du code avec l'aide du comité. Adopté par consensus, ce code sera la pierre angulaire, étayée par diverses normes techniques, d'un système national qui aidera les différents secteurs d'activité à se doter des codes de protection de la vie privée adaptés à leurs besoins particuliers.

Le Commissaire appuie avec enthousiasme la démarche de l'ACNOR à qui il a promis l'appui du Commissariat. Les organismes du secteur privé qui cherchent des solutions pratiques aux problèmes de la protection de la vie privée pourraient bien découvrir que l'approche de l'ACNOR est précisément celle qu'ils recherchaient.

La protection de la vie privée en milieu de travail

La protection de la vie privée en milieu de travail est elle aussi une question de plus en plus préoccupante, comme en témoigne la décision prise cette année par deux grandes compagnies (la Banque Toronto-Dominion et Exxon Canada) de mettre sur pied des programmes de dépistage des drogues. Dans les études déjà réalisées à ce sujet, le Commissariat a insisté sur l'utilité très limitée des programmes de ce genre, en concluant que les résultats susceptibles d'être obtenus

ne justifiaient pas les moyens intrusifs nécessaires. Ce qui s'est passé au cours de la dernière année nous laisse entendre que le moment est venu de chercher des moyens d'assurer le respect du droit individuel à l'intimité dans des secteurs d'activité où il y a des problèmes particuliers de sécurité ou d'une autre nature. Qu'on ne s'y trompe pas : le Commissaire ne prétend pas qu'on ne pourra jamais justifier un programme de dépistage, mais bien que, pour être acceptable, ces programmes doivent manifestement répondre à un besoin et être efficaces.

Une loi perfectible

La *Loi sur la protection des renseignements personnels* est en vigueur depuis maintenant neuf ans; soit depuis assez longtemps pour que des observateurs puissent poser des jugements provisoires sur son efficacité. Eh bien! Elle mérite de bonnes notes.

La doctrine des pratiques d'information équitables qui sous-tend la *Loi* s'est adaptée à des situations très variées dans un environnement en rapide évolution, et tout indique qu'elle sera vraiment durable. Chose certaine, on n'est pas encore arrivé à concevoir de meilleurs principes.

La principale lacune de la *Loi* est qu'elle ne s'applique qu'aux renseignements détenus par le gouvernement du Canada et par certains de ses organismes. Les pratiques d'information équitables qu'elle prévoit n'ont été reprises dans leurs propres lois que par quelques autres gouvernements seulement, et pas par le secteur privé, à quelques rares exceptions près. Nous pouvons donc affirmer que la plus grande partie - et de loin - des renseignements personnels détenus par des organismes et des entreprises canadiennes n'est toujours pas protégée.

À moins de réformes, la *Loi sur la protection des renseignements personnels* continuera d'être le plus important texte législatif du pays dans ce domaine, aussi bien parce que le gouvernement du Canada détient une masse énorme de renseignements personnels que parce qu'elle est l'étalon auquel les normes de protection des renseignements détenus dans d'autres secteurs peuvent être mesurées.

Bref, s'il est vrai que la Loi a une bonne fiche, il reste qu'elle doit constamment être réévaluée, non pas pour être modifiée de fond en comble, mais plutôt pour être «bonifiée», dans le jargon à la mode. Le Parlement l'a déjà soumise à un examen en 1986-1987, conformément au paragraphe 75(1). Mais six ans se sont écoulés depuis et le moment est peut-être venu de faire un autre examen.

Étonnamment, nous recommandons de renforcer les points forts de la Loi, c'est- à-dire la définition des renseignements personnels (article 3), le code des pratiques d'information équitables (articles 4 à 8) et la procédure d'accès aux renseignements personnels (articles 12 à 28).

Une nouvelle définition des «renseignements personnels»

Les architectes de la *Loi sur la protection des renseignements personnels* ne pouvaient pas prévoir l'émergence des techniques d'aujourd'hui quand ils ont proposé leur définition des renseignements personnels. Or, les progrès de la génétique, par exemple, confèrent un sens bien plus vaste à «des renseignements, quels que soient leur forme et leur support, concernant un individu identifiable» (définition des renseignements personnels, à l'article 3 de la Loi).

En effet, même la plus petite gouttelette de liquide ou le plus infime fragment de tissu tiré du corps d'un être humain recèle une masse de renseignements qui définissent avec des détails effarants les traits non seulement de l'individu lui-même, mais aussi ceux de ses ancêtres. Or, même si les alinéas 3*b*) et 3*d*) de la Loi portent sur les renseignements relatifs aux dossiers médicaux et aux groupes sanguins, il n'est pas clair que les renseignements concernant un individu identifiable qui sont contenus dans des prélèvements biologiques tombent sous le coup de l'article 3. Bien sûr, le Commissariat compte maintenir mordicus que oui, mais il suffirait de modifier l'article 3 en ce sens pour tuer dans l'oeuf toute controverse à ce sujet. En somme, nous recommandons qu'on reconnaisse clairement dans la définition donnée par la Loi que les renseignements contenus dans un échantillon génétique sont bel et bien des renseignements personnels aux fins de l'application de la Loi.

Certains prétendront que cette modification revient à modifier inutilement une définition déjà élégante. Pourtant, les données génétiques présentent de tels risques pour notre intimité qu'il est tout à fait justifié qu'elles soient mentionnées expressément dans la Loi.

Resserrement des conditions sur la communication des renseignements personnels

La protection des renseignements personnels repose sur les articles 7 et 8 de la Loi. Le principe fondamental à respecter est celui du consentement en connaissance de cause de l'individu concerné. Autrement dit, il est interdit d'utiliser ou de communiquer des renseignements personnels sans que l'individu concerné en soit informé et qu'il y consente.

La *Loi sur la protection des renseignements personnels* confirme une fois de plus que les règles doivent souvent tolérer des exceptions. Ces exceptions sont nécessaires pour concilier le droit de l'individu à la confidentialité des renseignements personnels le concernant et la responsabilité du gouvernement de gérer les affaires de l'État. Ainsi, il est raisonnable que des renseignements personnels soient divulgués sans le consentement de l'individu concerné pour satisfaire à des exigences juridiques ou pour qu'on puisse mener une enquête dans une procédure pénale.

Chose curieuse, l'un des points forts de la Loi est précisément une de ces exceptions, l'alinéa 8(2)*m*), qui autorise la communication de renseignements pour des raisons d'intérêt public. La Loi n'interdit pas ces communications-là et ne tente pas non plus de substituer des règles écrites détaillées au jugement réfléchi du responsable de l'institution. Elle établit simplement des principes d'une transparence manifeste garantissant que toutes les parties intéressées soient dûment informées et que le responsable exerce convenablement la latitude dont il dispose pour la communication des renseignements personnels. C'est le responsable de l'institution après tout, qui connaît le mieux ses documents; c'est donc à lui de concilier l'intérêt du public et le préjudice qu'il risque de faire subir à l'individu concerné.

Il reste que la plupart des communications sans consentement ne forcent pas le responsable de l'institution à se prévaloir de cette latitude, car il peut dans bien des cas déléguer la décision à son personnel. À cet égard, cet alinéa est perfectible. En effet, il ne faudrait pas qu'on délègue au personnel le pouvoir de communiquer des renseignements personnels pour des usages compatibles avec les fins auxquelles ils ont été recueillis ou préparés, pour les échanges d'information avec le gouvernement d'une province ou d'un État étranger ou pour la communication de renseignements à des organismes d'enquête, à des députés fédéraux, des chercheurs, des vérificateurs ou des associations d'autochtones. Étant donné qu'il s'agit dans ces cas-là de dérogations importantes au principe du consentement préalable de l'individu concerné, c'est le responsable de l'institution lui-même qui devrait être tenu de décider si la communication est justifiée.

Cette façon de procéder pourrait aussi éliminer une autre difficulté inhérente à la communication pour des usages compatibles avec les fins auxquelles les renseignements ont été recueillis. En effet, le paragraphe 9(1) de la Loi impose aux organismes fédéraux l'obligation d'aviser le Commissaire à la protection de la vie privée des cas où ils vont communiquer des renseignements personnels à des fins «compatibles» lorsque celles-ci ne figurent pas parmi celles énumérées dans *Info Source*. Or, le Commissariat n'a reçu et évalué que 18 avis de ce genre depuis sa création. L'expérience acquise grâce à l'instruction des plaintes et aux vérifications lui a appris qu'il y a régulièrement des communications à des fins «compatibles» sans que le Commissaire en soit avisé, comme il se doit. Si les plus hautes instances des organismes étaient tenues de rendre des comptes à ce sujet, la Loi serait respectée plus intégralement et avec plus de diligence.

Le Commissaire souhaite une amélioration des articles 7 et 8, mais il reste que la principale lacune du code des pratiques d'information équitables est qu'il ne prévoit aucun moyen pour un individu d'empêcher la communication de renseignements personnels qui le concernent avant qu'on ait pu juger de sa pertinence. Comme nous l'avons déjà précisé dans plusieurs rapports annuels, il est paradoxal que les gens à qui on refuse l'accès aux renseignements personnels qui les concernent puissent en appeler de cette décision devant les tribunaux, sans toutefois pouvoir en appeler de la décision d'un ministère ou d'un organisme de communiquer ces mêmes renseignements personnels à des tiers.

La *Loi à l'accès à l'information* prévoit un mécanisme servant à alerter les tiers - des compagnies, par exemple - quand des renseignements commerciaux délicats qui les concernent peuvent faire l'objet d'un échange d'information. La *Loi sur la protection des renseignements personnels*, elle, ne reconnaît pas de droit analogue aux individus quand des renseignements personnels délicats qui les concernent sont communiqués. Est-ce que les renseignements personnels ne méritent pas d'être au moins aussi bien protégés contre les divulgations abusives que les renseignements commerciaux?

Il est vrai que, dans les enquêtes concernant la sécurité nationale ou des procédures pénales, il n'est peut-être pas possible ou avisé de prévenir les individus concernés avant de communiquer ce genre de renseignements personnels. Toutefois, dans ces cas-là, la communication peut être étayée de pièces justificatives, afin que le Commissaire à la protection de la vie privée puisse juger si elle est justifiée.

Élargissement du critère du préjudice causé aux personnes concernées

La *Loi sur la protection des renseignements personnels* donne aux Canadiens une liste impressionnante de droits d'accès à des renseignements, mais elle donne aussi aux institutions gouvernementales un arsenal, que d'aucuns qualifieraient cyniquement d'inépuisable, de dispositions d'exception qui leur permettent d'en faire fi. Ces exceptions-là ne sont pas déraisonnables si elles peuvent être étayées par un raisonnement clair et logique, et c'est le cas, la plupart du temps. Ainsi, qui voudrait que des terroristes n'aient qu'à demander à consulter les documents personnels qui les concernent pour savoir que la police est sur le point de leur mettre la main au collet?

Néanmoins, certaines exceptions vont peut-être trop loin. Ainsi, en vertu de l'article 19, de l'alinéa 22(1)*a*) et du paragraphe 22(2), les organismes gouvernementaux peuvent - ou doivent - refuser de communiquer des renseignements personnels sans être tenus de démontrer que cette communication risquerait de porter préjudice à quelqu'un. Ces trois dispositions visent respectivement les renseignements personnels obtenus d'autres gouvernements, ceux qui sont utilisés pour des activités destinées à faire respecter les lois et enfin ceux qui ont été obtenus par la GRC dans l'exercice de fonctions de police provinciale ou municipale. Les renseignements personnels protégés par le secret professionnel qui lie un avocat à son client (article 27) font eux aussi l'objet d'une exception analogue.

L'alinéa 22(1)*a*) est certainement l'aspect le plus choquant car il autorise le gouvernement à refuser l'accès à des renseignements personnels préparés «au cours d'enquêtes licites ayant trait aux activités destinées à faire respecter les lois fédérales ou provinciales», à condition que l'enquête soit menée par un «organisme d'enquête». Il y a neuf organismes d'enquête énumérés dans la réglementation découlant de la *Loi sur la protection des renseignements personnels*. Autrement dit, cette exception équivaut à donner carte blanche à ces organismes, qui peuvent refuser de donner l'accès aux Canadiens à des renseignements personnels qui les concernent, pour toutes les raisons imaginables, voire sans raison. Aucun organisme ne devrait avoir le droit de refuser cet accès sans justification.

En fait, on n'a généralement pas abusé de cette exception. Par exemple, alors qu'on pourrait s'attendre à ce que la GRC l'invoque souvent, elle ne le fait que rarement, préférant se fonder sur d'autres dispositions de la Loi. Néanmoins, certains cas ont clairement révélé comment l'alinéa peut être mal appliqué.

En voici un exemple frappant. Le directeur des Enquêtes et Recherches de Consommation et Affaires commerciales Canada avait enquêté sur une plainte dans laquelle on avait accusé la Tribune de la presse du Parlement d'avoir violé les règles fédérales sur la concurrence en rejetant une demande d'adhésion. L'enquête du ministère n'a révélé aucune violation des règles établies, mais lorsque le plaignant a poursuivi sa démarche en invoquant la Loi pour obtenir copie des opinions exprimées par les membres de la Tribune sur sa demande, le ministère a refusé de les lui communiquer, en vertu de l'alinéa 22(1)*a*). Étant donné que l'enquête avait été exhaustive, le Commissaire s'est dit d'avis qu'il n'y avait aucune raison valide pour que la demande d'information ait été rejetée. Néanmoins, le ministère n'a rien voulu entendre et le Commissaire n'a rien pu faire de plus, puisque le ministère avait parfaitement le droit de refuser d'obtempérer en se prévalant de la Loi.

C'est ce genre d'exception «générale» qu'il faudrait abroger, car elle s'est révélée inutile même dans des situations aussi délicates que celles d'enquêtes policières. Sous sa forme actuelle, l'alinéa 22(1)*a)* est simplement une échappatoire commode pour des bureaucrates non désireux de se donner la peine de justifier leurs décisions. Par contre, l'alinéa 22(1)*b)*, qui impose comme condition de refus de communiquer les renseignements que leur divulgation risque d'avoir des conséquences néfastes, pose un principe raisonnable permettant aux institutions gouvernementales de gérer efficacement leurs programmes.

La portée de cette exception explique pourquoi le Commissaire accueille avec quelque réticence les ajouts à la liste des organismes d'enquête. Au cours de l'année, on l'a informé qu'on envisageait la création de trois nouveaux organismes de ce genre. Loin de nous l'idée de chercher noise aux organismes en question; c'est plutôt avec la notion même d'un organisme d'enquête que nous avons maille à partir. Les autres exceptions donnent aux responsables des institutions toute la latitude dont ils ont besoin, à condition qu'ils tiennent compte du risque de porter préjudice aux intéressés. Pour le moment, le Commissariat participe aux travaux d'un groupe d'étude qui analyse cette exception, son utilisation et quelques possibilités de rechange pour l'avenir.

L'absurde érigé en système

La Loi a une dernière lacune qu'il faut dénoncer dans ce rapport.

C'est l'article 16, qui permet aux institutions fédérales de refuser de confirmer ou de nier l'existence de renseignements personnels demandés. Pour la plupart d'entre nous, les exceptions à la règle limitent bien assez le droit général d'accès à l'information. Or, l'article 16 va beaucoup plus loin qu'autoriser un simple refus de communiquer des renseignements personnels.

La doctrine du refus de confirmer l'existence de renseignements quelconques ou de la nier est profondément ancrée dans la mentalité des organismes canadiens oeuvrant dans les secteurs de la sécurité et de la police; l'article 16 nous semble en être le corollaire juridique. Si désagréable que cette doctrine soit dans une société libre et démocratique, il peut être nécessaire que nous la tolérions, dans l'intérêt public. Néanmoins, invoquer cet article en même temps qu'une disposition d'exception quelconque, sauf celle qui porte sur les activités des forces de sécurité et des forces policières (articles 21 et 22), c'est de toute évidence porter une atteinte inacceptable à un droit d'accès déjà trop limité et trop fragile. La Loi devrait être modifiée afin de limiter cette autorité à la sécurité nationale et aux enquêtes criminelles.

Nos droits à l'intimité sont d'autant plus menacés que, même si le Commissaire à la protection de la vie privée peut instruire des plaintes fondées sur cet article, il lui est interdit de divulguer les renseignements obtenus au cours de son enquête, voire de faire état de l'existence des renseignements personnels demandés!

Si le Commissaire ne peut résoudre la plainte, il plonge dans l'absurde. Le seul fait de renvoyer l'affaire à la Cour fédérale l'expose à risquer de révéler l'existence des renseignements et, par conséquent, d'enfreindre sa propre Loi. Bref, il faut ajouter à la Loi un mécanisme permettant au Commissaire en dernier recours de renvoyer ces plaintes aux tribunaux.

Le dépistage génétique

Il est facile d'oublier les implications, pour la protection de la vie privée, de technologies que bien d'entre nous ne comprenons pas encore parfaitement. À cet égard, rien n'est aussi dangereux que le dépistage génétique.

Les progrès de la technologie génétique nous permettront certainement d'élucider des mystères médicaux et, ainsi, de prévenir de nombreuses maladies et d'en traiter efficacement bien d'autres. La technologie nous a déjà permis d'identifier de nombreux traits ou désordres génétiques et parfois même de prédire exactement notre avenir génétique. Ce sont de bonnes nouvelles, mais toute médaille a son revers. En effet, les gènes peuvent révéler des secrets bien gardés sur nos caractéristiques physiques et psychologiques, et ces secrets, nous ne voulons peut-être pas que d'autres les connaissent, même si nous voulons les connaître nous-mêmes! Réduire l'essence même de l'humanité à l'écheveau compliqué des molécules d'ADN (autrement dit à la structure même de nos gènes), c'est une attaque contre notre intimité que bien peu d'entre nous sommes prêts à tolérer.

Les gouvernements - ou qui que ce soit d'autre - ont-ils le droit de recueillir des renseignements génétiques personnels «dans l'intérêt public» avec ou sans notre consentement? Devrions-nous avoir le droit de protéger nos gènes des inspecteurs de l'État ou du secteur privé?

Cette année, le Commissariat a publié *Le dépistage génétique et la vie privée*, troisième volet de sa trilogie sur le dépistage biomédical (les deux premiers portaient l'un sur le dépistage du VIH et du SIDA et l'autre sur le dépistage antidrogue). Le troisième rapport est un examen des questions découlant du développement rapide de la technologie du dépistage génétique, et notamment de plusieurs de ses utilisations actuelles ou potentielles. Les tests de dépistage pourraient être conçus de façon à sélectionner des employés génétiquement optimaux ou à contrôler les effets des dangers pour leur santé auxquels ils sont exposés en milieu de travail, à déterminer l'admissibilité à des prestations ou à des services comme l'assurance, à diagnostiquer ou à prédire des troubles dans le cours normal de soins médicaux de routine ou de la reproduction humaine (dépistage préconception, prénatal et néonatal) et à permettre aux médecins légistes de produire des éléments de preuve plus précis.

Au Canada, le dépistage génétique semble jusqu'à présent avoir été limité à trois domaines : les techniques de reproduction humaine, les soins médicaux courants et les procédures médico-légales. Toutefois, la mise au point de tests moins coûteux et générant plus de renseignements renforcera presque à coup sûr l'intérêt pour ce genre de dépistage. Et les gouvernements ne seront pas les seuls à s'immiscer dans notre vie privée; dans le secteur privé, les employeurs et les assureurs, par exemple, seront de plus en plus séduits par les prétendus avantages d'un dépistage génétique capable de les aider à devancer la concurrence.

Les gouvernements seront peut-être tentés de surmonter de graves appréhensions d'ordre éthique pour appliquer les connaissances acquises en génétique afin de favoriser l'eugénisme. Chose certaine, le monde d'aujourd'hui n'est pas exempt de pressions de ceux qui préconisent une société «optimisée». Dans le secteur privé, la génétique pourrait être utilisée comme moyen d'identification des personnes génétiquement «inférieures». Pour les infortunés classés dans ce «sous-ordre», l'accès à l'emploi ou aux services risquerait d'être sérieusement réduit.

Autant dans le secteur public que dans le secteur privé, des caractéristiques génétiques indépendantes de notre volonté deviendraient des facteurs déterminants de la façon dont on nous permettrait de vivre notre vie, sans beaucoup d'égards pour les êtres humains que nous sommes tous, au-delà de nos gènes.

Le Commissariat a été effaré par les possibilités de prolifération du nombre et des types d'intrusions rendus possibles par les progrès de la technologie génétique. Par conséquent, il s'est prononcé dans son rapport contre le dépistage génétique obligatoire (et, dans certains cas, volontaire) dans plusieurs situations. Il a aussi pressé le gouvernement fédéral d'étudier l'étendue du dépistage génétique au Canada ainsi que les utilisations futures les plus probables de cette technologie.

Le rapport contient plusieurs recommandations expresses, à savoir :

- chacun devrait raisonnablement être en droit de s'attendre à ce que son patrimoine génétique soit gardé secret;

• les gouvernements ne devraient recueillir des renseignements génétiques personnels que si des dispositions législatives précises les y autorisent;

• ni les gouvernements, ni le secteur privé ne devraient obliger les gens à connaître leurs traits ou leurs affections génétiques;

• les employeurs devraient se voir interdire l'imposition de tests de dépistage génétique obligatoires dans le contexte de l'emploi, que ce soit pour identifier des traits génétiques indésirables chez leurs employés et chez les candidats postulant des emplois ou pour identifier des changements génétiques résultant de l'exposition à diverses conditions en milieu de travail; seul le dépistage sur une base absolument volontaire devrait être autorisé;

• les dispensateurs de services ou de prestations ne devraient pas être autorisés à imposer des tests obligatoires de dépistage génétique pour déterminer l'admissibilité des postulants;

• les gouvernements ne devraient pas recueillir de renseignements génétiques personnels portant sur le processus de reproduction;

• les gouvernements ne devraient pas recueillir de renseignements génétiques personnels portant sur les soins médicaux courants;

• les gouvernements devraient limiter l'analyse pathologique de l'ADN dans les enquêtes criminelles aux seules fins d'identification des criminels ou d'exonération des suspects;

- les gouvernements ne devraient pas établir de bases de données génétiques contenant des éléments d'identification ou des banques de matériel génétique pour l'ensemble de la population, aux fins du système de justice pénale.

Le rapport n'est guère qu'un survol du dépistage génétique, mais le Commissaire espère qu'il stimulera la réflexion et l'action avant que de puissants intérêts du secteur public ou du secteur privé ne nous transforment tous, des êtres humains que nous avons toujours été, à la simple somme de nos pièces génétiques.

Les appareils de télécommunication : c'est jouer avec la vie privée

Les lecteurs assidus des rapports annuels se rappellent peut-être que l'ancien Commissaire à la protection de la vie privée s'inquiétait des dangers de la nouvelle technologie des télécommunications pour la vie privée (Rapport annuel 1989-1990, p. 32). Le Commissaire s'inquiétait particulièrement du nouveau Service de gestion des appels (SGA) de Bell Canada, et plus particulièrement de l'Afficheur. Le CRTC a depuis approuvé le service offert par Bell Canada, et la plupart des autres compagnies de téléphone ont maintenant des services analogues.

L'Afficheur n'est qu'un des éléments de la nouvelle technologie téléphonique. Une grande partie des nouveaux services ne sont pas dus à l'amélioration des postes de téléphone, mais bien à la puissance des ordinateurs de commutation. Bien entendu, les usagers ont besoin de téléphones spécialement équipés afin de pouvoir voir et noter le numéro de téléphone affiché avant de décrocher.

Cela peut leur assurer une certaine protection contre les appels de harcèlement. Mais cela s'effectue aussi aux dépens des correspondants, qui ont le droit tout aussi légitime de ne pas souhaiter qu'on connaisse leur numéro de téléphone ou qu'on en prenne note.

Ce désir ou besoin d'anonymité est bien naturel pour les gens qui appellent des lignes ouvertes en cas de crise ou pour les bénévoles qui doivent souvent retourner des appels depuis leur domicile. Dorénavant, bien des gens - des psychiatres aux agents de probation et des politiciens aux policiers en civil - risquent de ne plus pouvoir téléphoner de chez eux, de peur que leur numéro de téléphone ne soit affiché et pris en note.

En outre, bien des gens s'inquiètent de l'utilisation commerciale qu'on pourrait faire de leur numéro de téléphone. Quiconque appelle une entreprise s'expose désormais à voir son numéro de téléphone pris en note, puis à être rappelé dans le contexte de campagnes de démarchage. De plus, grâce aux bottins téléphoniques inversés (dans lesquels les abonnés sont inscrits dans l'ordre de leurs numéros de téléphone) on peut facilement trouver les noms et les adresses.

C'est payer bien cher les quelques avantages du SGA que d'y sacrifier la vie privée de tous les usagers. De plus, facturer les abonnés pour **prévenir** l'affichage de leurs numéros, signifie que la protection de la vie privée est à vendre, et certains n'auront pas les moyens de s'offrir ce luxe.

Bref, toutes ces craintes sont fondées, et les solutions pratiques sont difficiles à trouver. Le SGA peut varier selon la compagnie de téléphone, de sorte qu'on aboutit avec une kyrielle de mesures de protection disparates. Certaines compagnies autorisent les correspondants qui appellent à bloquer l'affichage du numéro pour tous les appels faits sur leur ligne (ou seulement pour certains appels), mais elles leur font payer ce service. Certaines autres ne facturent rien pour bloquer l'affichage. D'autres encore offrent une sorte d'encryptage qui brouille le numéro. De plus, presque toutes les compagnies ont une solution particulière à l'intention des refuges pour femmes.

La plus récente décision rendue à l'égard du SGA émane du Manitoba Public Utilities Board, qui a approuvé la demande de projet pilote de Manitoba Telephone Services à condition que tous les abonnés de la compagnie aient droit à un service gratuit de blocage des appels. Les autorités manitobaines ont aussi exigé un blocage gratuit de la ligne pour les refuges et pour les victimes de voies de fait. Toutefois, elles n'ont pas approuvé le service de retour d'appel, qui conserve les numéros des correspondants ayant fait des appels restés sans réponse pour les afficher plus tard sur commande.

Fait important, le CRTC a récemment annoncé bien après la fin de notre exercice, que les entreprises de téléphone sous sa juridiction doivent offrir gratuitement le service de blocage des appels.

Cela dit, le Canada n'est pas le seul pays à s'efforcer de trouver des solutions appropriées aux problèmes causés par le progrès technologique. Aux États-Unis, le débat fait rage depuis que le New Jersey a introduit un service analogue en 1987, et l'on compte parmi les intervenants des commissions de services publics, des législatures d'État, la législature fédérale et même les tribunaux.

Les solutions vont d'un extrême à l'autre. Au New Jersey, on n'offre aucun service de blocage. En Pennsylvanie, l'État a jugé le SGA illégal, puisqu'il contrevient à sa loi sur l'écoute électronique.

Au Texas, on voudrait que l'usager paye pour avoir l'affichage et dans un cas récent, un juge siégeant dans une affaire de droit administratif en Californie a proposé que la Commission des services publics de l'État interdise l'affichage du numéro de téléphone du correspondant qui appelle, parce que cet affichage n'est pas d'intérêt public et viole à la fois les dispositions de l'État et du gouvernement fédéral sur le droit à l'intimité garanti par la Constitution.

D'autres États offrent le blocage de l'affichage gratuit par appel, une facturation par ligne ou encore le blocage de l'affichage gratuit par appel **et** par ligne. Quand le débat battait son plein, une compagnie de téléphone a même offert un service permettant aux usagers de refuser automatiquement les appels bloqués. Les possibilités sont légion.

Bref, le débat a focalisé l'attention du public sur la protection de la vie privée. Néanmoins, ce qui est sans doute plus inquiétant, c'est le fait qu'on sait bien que ces services ne sont qu'un début, l'un des premiers éléments d'un système intelligent de réseaux en expansion croissante. Ce système offrira bientôt des réseaux de communication personnels où les usagers auront un numéro de téléphone personnel leur vie durant, des services de composition et des téléphones à écran. La technologie évolue si vite que ni les ingénieurs, ni les décideurs n'ont le temps de réfléchir à ses impacts sociaux. Chaque nouvelle découverte sape ou perce les barrières érigées si laborieusement contre la précédente pour protéger notre vie privée.

De toute évidence, les maigres ressources du Commissariat à la protection de la vie privée ne lui permettent pas de se maintenir au diapason de chaque nouvelle merveille technique; il n'a ni les compétences, ni l'effectif nécessaire. Néanmoins, le Commissaire tient à trouver des solutions pratiques durables.

L'approche adoptée par l'État de New York présente beaucoup d'intérêt. En effet, la Commission des services publics de l'État s'est donné huit principes généraux de protection de la vie privée dans le domaine des télécommunications. Ceux-ci précisent que les compagnies de télécommunications devraient reconnaître explicitement le droit à la vie privée de leurs clients, de sorte que ceux-ci ne devraient pas avoir à payer davantage pour maintenir la protection dont ils bénéficient actuellement. Les clients devraient être informés de toute utilisation qu'on se propose de faire des renseignements qui les concernent et ils devraient y consentir, s'ils le désirent, en toute connaissance de cause.

Le Commissariat et le ministère des Communications étudient actuellement toute la question de l'impact des télécommunications sur la vie privée et se penchent sur les solutions possibles.

Nouvelle Loi sur les télécommunications

Le projet de *Loi sur les télécommunications* pourrait être un pas dans la bonne direction, puisque le Parlement y reconnaît les dangers de la technologie des télécommunications pour la vie privée. La Loi a notamment pour objectif

> "...satisfaire les exigences économiques et sociales - notamment quant à la protection de leur vie privée - des usagers des services de télécommunication..."

De plus, la Loi autorise le gouvernement et le CRTC à interdire les intrusions comme les appels téléphoniques et les messages télécopiés indésirés dans la vie privée des citoyens.

Le Commissariat a l'intention de suivre l'évolution de ce projet de loi à la Chambre, pour s'assurer que les mesures de protection de la vie privée ne sont pas touchées. Et l'on se demande si les dispositions prises vont assez loin. La Loi ou ses règlements devraient mettre en évidence les normes qui s'appliquent à la vie privée que les services de télécommunications devraient rencontrer.

Et la saga du NAS continue...

Née sans NAS

La résistance aux demandes de divulgation du numéro d'assurance sociale (NAS) a pris une tournure inhabituelle cette année, quand un couple de l'Île-du-Prince-Édouard a refusé de demander un NAS pour son bébé.

Le service des statistiques vitales de la province exige que tous les nouveau-nés se fassent attribuer un NAS, utilisé comme numéro d'identité pour le Régime provincial de paiement des services de santé. Le couple a demandé une exemption qui lui a été refusée, et le ministère provincial de la Santé a réagi en refusant d'honorer toutes les demandes de remboursement de frais médicaux de leur enfant, parce que celle-ci n'avait pas de NAS.

Le couple a traîné l'affaire devant les tribunaux, en alléguant qu'obliger le bébé à avoir un NAS (et rejeter leurs demandes de remboursement de frais médicaux) viole plusieurs dispositions de la *Charte canadienne des droits et libertés*. Selon les parents, l'enfant n'a aucune obligation légale d'obtenir un NAS avant de commencer à occuper un emploi assurable. En outre, en rejetant les demandes de remboursement de frais médicaux, les autorités provinciales ont contrevenu aux dispositions de la *Charte* sur la protection contre les fouilles et saisies abusives et elles ont refusé au bébé le droit à l'égalité devant la loi; de plus, obliger un bébé à avoir un NAS porte atteinte au droit de chacun à une protection raisonnable de sa vie privée.

L'affaire intéresse le Commissariat, même si elle est bien loin de la *Loi sur la protection des renseignements personnels*. Néanmoins, elle soulève une importante question pour la protection de la vie privée : quel programme ou quelle activité d'Emploi et Immigration Canada (ministère responsable de l'attribution du NAS) l'autorise à attribuer ce numéro à des nouveau-nés?

Le NAS a été créé aux fins de l'assurance-chômage et du Régime de pensions du Canada; par la suite, Revenu Canada a été autorisé à l'utiliser pour les déclarations d'impôt sur le revenu des particuliers. Ces dernières années, le gouvernement fédéral a adopté une politique - louangée par le Commissaire - qui a mis fin à de nombreuses utilisations abusives du NAS dans l'administration fédérale. Toutefois, pour attribuer un NAS aux nouveau-nés, il semble qu'EIC se fonde toujours sur une entente fédérale-provinciale conclue en 1970, soit bien avant que le gouvernement n'ait pris des mesures pour protéger la vie privée.

Le Commissaire a demandé à Emploi et Immigration de lui dire s'il existe une relation directe entre ses programmes et le fait qu'il assigne un NAS aux fins de l'enregistrement des naissances. S'il n'y a pas de relation de ce genre, il compte presser EIC de repenser son entente avec les autorités provinciales de l'Île-du-Prince-Édouard, prenant en considération à la fois la *Loi sur la protection des renseignements personnels* et la politique actuelle du gouvernement fédéral, qui limite l'utilisation du NAS à une courte liste de programmes sociaux.

Que celui qui est sans péché lance la première pierre : renumérotation de la Fonction publique

La politique de l'administration fédérale de réduire son utilisation du NAS a d'importantes conséquences; ainsi il lui faut renuméroter quelque 310 000 fonctionnaires, militaires et membres de la GRC.

Approvisionnements et Services Canada, (responsable des bases de données de la rémunération et des dossiers), commencera en janvier 1993 à attribuer un nouveau code d'identification de dossier personnel (NIP). Chaque membre de la Fonction publique se verra attribuer deux numéros, un NIP et un autre numéro qu'il pourra divulguer à des tiers, par exemple à ses institutions bancaires, compagnies d'assurance et syndicats. Ce deuxième numéro garantira la confidentialité du NIP, tout en permettant à l'employeur de relier à l'intéressé les opérations que celui-ci a faites avec des tiers.

Les gens ne sont pas encore tout à fait sûrs quand une demande de divulgation du NAS est justifiée. Par exemple, les responsables des programmes d'examen des connaissances linguistiques de la Commission de la Fonction publique demandent encore leur NAS aux fonctionnaires, et les syndicats de la Fonction publique continuent eux aussi à s'en servir pour leurs listes de membres. Ces demandes-là sont justifiées. Néanmoins, une fois la renumérotation des postes menée à bien, le Commissaire recommandera aux fonctionnaires et autres membres de l'administration fédérale de ne pas divulguer leur nouveau NIP.

Le NAS ou gare!

Le Commissariat a été saisi de ce qui semble être une utilisation abusive du NAS à la nouvelle banque automatisée de renseignements sur les emplois d'Emploi et Immigration à St. John's (Terre-Neuve). Il s'agit d'un projet pilote grâce auquel les personnes qui recherchent un emploi peuvent consulter une liste informatique des postes disponibles afin de choisir ceux qui correspondent à leurs intérêts et à leurs aptitudes. Le système offre des possibilités accrues au public et libère du personnel d'EIC, qui peut alors vaquer à d'autres tâches.

Toutefois, quelqu'un s'est plaint en disant qu'il n'avait même pas pu voir la liste sans donner son NAS. Selon le plaignant, vu que n'importe quel passant peut consulter sur papier les offres d'emploi disponibles, exiger la production d'un NAS pour donner accès à une liste informatique était exagéré et même inutile, puisqu'il ne réclamait pas de prestations d'assurance-chômage.

Il semble qu'EIC ait demandé le NAS pour mesurer à la fois l'efficacité de son système et sa capacité de placer des prestataires de l'assurance-chômage. Quand le Commissariat le lui a demandé, EIC a reconnu que son système devrait être également accessible aux gens qui ne touchent pas de prestations d'assurance-chômage.

Depuis, le système a été modifié. Au départ l'écran affiché informe les utilisateurs que l'accès au système est libre. Les prestataires de l'assurance-chômage ont le choix d'y introduire leur NAS, de façon que le Centre d'emploi du Canada ait une indication de leur recherche d'emploi. Le changement sera incorporé dans le nouveau système national de banque d'emplois.

Derniers progrès technologiques

L'an dernier, le Commissaire faisait état dans son rapport des projets d'Emploi et Immigration Canada (EIC) de mettre à profit les dernières découvertes informatiques pour mieux servir son énorme clientèle. EIC avait lancé deux projets pilotes, l'un faisant appel à des cartes à mémoire et l'autre à un Système de réponse vocale automatisée (SRVA).

EIC n'est pas le seul organisme fédéral qui ait songé à l'informatique pour améliorer son service. Anciens combattants Canada a déjà fait des essais avec des cartes à mémoire dans le but d'améliorer ses systèmes d'envoi et de facturation de médicaments sur ordonnance aux anciens combattants. En outre, Revenu Canada étudie la possibilité de faire utiliser ces cartes par les voyageurs pour déclarer des marchandises ou payer des droits aux postes de douane.

Plusieurs ministères collaborent actuellement en vue de mettre au point des cartes à mémoire rendant possible la téléconsultation des ordinateurs gouvernementaux. Cela permettrait aux gens qui ont un ordinateur personnel chez eux de communiquer par téléphone avec les ordinateurs des organismes gouvernementaux.

Bien entendu, à l'instar de bien d'autres applications de la technologie moderne des communications, ces projets ont des implications pour la vie privée.

La carte à mémoire ressemble à une carte bancaire ou à une carte de crédit, mais avec une différence fondamentale. Ces cartes sont porteuses d'une puce de circuits intégrés qui leur donne la capacité de traiter des données et d'en emmagasiner. Grâce aux puces et à la présentation numérique des renseignements, les cartes peuvent aussi contenir une photographie invisible du porteur, voire ses empreintes digitales. Elles pourraient être utilisées pour fournir des services bancaires, téléphoniques et médicaux et pour donner à leurs utilisateurs l'accès à tout un réseau d'ordinateurs.

Besoins de protection de la vie privée

De toute évidence, les cartes à mémoire représentent un important progrès technique susceptible d'améliorer le service à la clientèle des ministères et organismes gouvernementaux et de les aider à limiter leurs frais. C'est particulièrement vrai dans le cas d'organismes comme EIC, qui doivent suivre une clientèle assez nombreuse, créditer des déductions et verser des prestations.

Néanmoins, les organismes gouvernementaux et leurs clients devraient pouvoir jouir des avantages du progrès sans sacrifier pour autant le contrôle de l'individu sur les renseignements personnels qui le concernent. En fait, les cartes à mémoire pourraient bien devenir la carte d'identité universelle à laquelle les Nord-Américains résistent si farouchement. Leur invention risque de transformer radicalement la relation entre l'individu et l'État.

Si nous voulons éviter cela, nous devons d'abord commencer par assurer la transparence des systèmes pour les clients. Les porteurs de carte doivent connaître leurs droits intrinsèques quand ils se servent de leur carte; ils doivent aussi savoir quels renseignements la carte contient, comment elle sera utilisée et quels sont les risques.

Les gens devraient avoir le droit de refuser la carte sans risquer de limiter leur accès aux services. De même, les détenteurs de carte ne devraient pas être avantagés par rapport à ceux qui refusent d'en avoir une.

Enfin, les systèmes et leurs participants doivent respecter à la fois la législation sur la protection de la vie privée et les principes d'éthique fondamentaux régissant la collecte, le traitement et la divulgation des renseignements personnels.

Les risques de sécurité inhérents aux projets pilotes inquiétaient tellement le Commissaire que son personnel a été invité à participer à deux groupes de travail du gouvernement fédéral, l'un chargé d'étudier les applications de la nouvelle technologie et l'autre responsable de l'établissement de normes de téléconsultation des systèmes informatiques.

Le groupe chargé des applications, qui a pour objectif ultime d'établir des normes et des lignes directrices pour toutes les applications futures des cartes à mémoire dans l'administration fédérale, définira comment les institutions gouvernementales pourraient utiliser ces cartes et dans quel contexte elles devraient être employées. Les membres de ce groupe comptent des représentants d'organismes fédéraux comme Santé et Bien-être social Canada, Approvisionnements et services Canada, la GRC et Anciens combattants Canada, de même que des ministères de la Santé du Québec et de l'Ontario.

Le Commissariat est aussi représenté au groupe d'intérêts spéciaux chargé des normes sur la téléconsultation de systèmes informatiques. Étant donné que de nombreux organismes gouvernementaux ont des intérêts communs en matière d'accès, ils partagent les frais de recherche et de développement et contribuent à l'établissement de ces normes communes.

Le projet SRVA

Dans le rapport annuel de l'an dernier, (page 63), le Commissaire avait décrit une des lacunes du projet pilote de Système de réponse vocale automatisée qu'Emploi et Immigration Canada (EIC) avait amorcé à Québec. Ce passage du rapport se terminait sur une mauvaise note, puisque le projet semblait trop avancé pour être modifié. Toutefois, EIC a rédigé une nouvelle conclusion et le Commissaire en est plus que ravi.

Le Système permettait aux usagers du téléphone à clavier de communiquer par téléphone avec un ordinateur pour obtenir de l'information d'ordre général sur leurs demandes de prestations d'assurance-chômage. Par exemple, ils pouvaient confirmer si leur demande avait été acceptée et quand ils commenceraient à toucher leurs prestations. Les intéressés s'identifiaient en donnant leur numéro d'assurance sociale (NAS) et leur date de naissance. Le Commissariat avait été informé de l'existence du système par une station de radio locale, qui lui avait demandé si cette utilisation du NAS était autorisée.

Il est certain qu'EIC peut se servir du NAS pour identifier les prestataires de l'assurance-chômage : le NAS a été conçu expressément à cette fin. Cependant, le Commissaire s'inquiétait du manque de protection de la combinaison NAS-date de naissance. Le Commissariat a discuté du problème avec les représentants d'EIC, qui ont reconnu que ces deux types de renseignements personnels sont très répandus, de sorte qu'ils ne constituent pas un code d'accès très bien protégé. Malheureusement, le projet pilote avait déjà gagné London et Peterborough et il semblait trop tard pour le modifier.

Néanmoins, les concepteurs de systèmes d'EIC se sont montrés sensibles aux inquiétudes du Commissaire. Ils ont profité du projet pilote de Peterborough pour tester un nouveau code téléphonique d'accès à quatre chiffres semblable à un numéro bancaire.

Il semble bien que l'expérience ait été couronnée de succès et le nouveau code sera utilisé dans le programme national. EIC donnera ce numéro code aux prestataires pour qu'ils puissent s'identifier lorsqu'ils feront des demandes de renseignements par téléphone. Les prestataires pourront aussi choisir leur propre numéro de code, s'ils le désirent.

Le Commissaire applaudit à la rapidité de réaction d'EIC et à sa sensibilité à protéger sa clientèle.

Couplage de données

Dans ce domaine, la meilleure nouvelle de l'année, c'est qu'on a signalé au Commissariat très peu de nouveaux cas de couplage de données. Le Commissaire n'a reçu que trois avis au cours de l'année écoulée, tous provenant d'Agriculture Canada.

Le Commissaire ne voudrait pas sembler trop soupçonneux. Néanmoins, il serait vraiment crédule s'il souscrivait à l'idée qu'un seul organisme fédéral sur plus de 150 qui sont soumis à la politique de couplage des données du gouvernement aurait commencé en 1991-1992 à coupler des dossiers distincts.

La politique de couplage interdit de relier des bases de données informatiques susceptibles de produire des dossiers détaillés (appellés «superdossiers») sur les particuliers. Les organismes fédéraux doivent aussi soumettre au Commissaire leurs propositions de ce

genre au moins 60 jours à l'avance. Le Commissaire évalue alors la validité du couplage en fonction d'une série de critères et se fait le défenseur de ceux qui font l'objet des dossiers visés. Il s'agit en somme d'empêcher le gouvernement d'enfreindre, par souci d'efficience, les droits des gens à la protection des renseignements personnels les concernant.

C'est une politique admirable, mais peut-être pas très efficace. Seulement 22 organismes fédéraux ont dans le répertoire des renseignements fédéraux, *Info Source*, des inscriptions décrivant quelque chose qui ressemble - même de loin - à un couplage de données. Il est bien connu que certains ministères rangent les couplages sous des rubriques plus anodines "d'utilisation" ou de "divulgation". D'autres organismes ne reconnaissent l'existence d'un couplage que lorsqu'il y a une liaison entre leurs données et celles d'un organisme distinct, ce qui est contraire à la politique qui s'applique clairement aussi au couplage de fichiers de différents programmes d'un même organisme.

Tout ce que le Commissaire a vu jusqu'à présent l'amène à conclure que le couplage de données informatiques est un phénomène courant au gouvernement, particulièrement dans le cas des programmes sociaux, des activités d'application de la loi et de recherche de renseignements et du système de justice pénale. Les fonctionnaires sont-ils capables d'identifier les couplages de données? Sont-ils au courant de la politique? La considèrent-ils simplement comme un obstacle à contourner?

Bref, le Commissaire presse le Conseil du Trésor d'enquêter. Cela dit, ses équipes de vérification de l'observation ont ajouté le couplage de données à leur liste de critères de vérification.

Couplages de données agricoles

En toute justice, il faut reconnaître qu'Agriculture Canada a scrupuleusement respecté la politique sur le couplage de données. Dans le premier avis il l'a informé que la nouvelle *Loi sur la protection du revenu agricole* l'autoriserait à coupler les données sur les agriculteurs tirées du compte de stabilisation du revenu avec les données sur les revenus de Revenu Canada.

Grâce à ce couplage, les prestations versées aux agriculteurs par ce programme seront calculées en fonction de renseignements exacts sur leurs revenus, leurs dépenses et leur production. La Loi donne à Agriculture Canada le pouvoir légal de faire les couplages nécessaires, en l'autorisant à utiliser le numéro d'assurance sociale des intéressés.

Saisies pour besoins familiaux : Agriculture Canada a aussi avisé le Commissaire de son intention de coupler les données tirées du Programme de stabilisation concernant le grain de l'Ouest avec celles du ministère de la Justice, pour qu'il soit possible de saisir les paiements versés par ce programme aux agriculteurs qui ne paient pas leurs pensions alimentaires et autres types de contributions aux besoins de leur famille. En réalité, il n'était pas nécessaire que le ministère soumette sa proposition au Commissariat, puisque le Parlement a pris un règlement, en vertu de la *Loi d'aide à l'exécution des ordonnances et des ententes familiales*, afin d'autoriser des retenues à même le Programme de stabilisation.

Un complément d'information s'impose : le Commissariat a été enfin avisé de l'intention d'Agriculture Canada de coupler les données des dossiers du Bureau d'examen de l'endettement agricole avec ceux du ministère de l'Agriculture du Québec, afin de faciliter le fonctionnement d'un nouveau programme de subvention des exploitants de parcs d'engraissement de bovins et de médiation avec les créanciers des agriculteurs. Toutefois, le Commissariat n'a pas reçu assez de détails pour évaluer ce couplage.

La division des plaintes

Le Bureau a reçu 1 402 nouvelles plaintes cette année en comparaison de 1 239 l'an dernier—une augmentation de 13 pourcent. Cette augmentation suit le même scénario que celui établi par le bureau depuis sa création en 1983. Ce qui diffère est la diminution du nombre de dossiers complétés. Les enquêteurs ont fermés 782 cas, dont 269 étaient bien fondés, 448 étaient non bien fondés et 65 ont été abandonnés.

Le recensement de 1991

Au cours de la dernière année, ce dossier a retenu beaucoup de notre attention; nous avons enquêté sur 34 plaintes au sujet du recensement de 1991. Plusieurs plaignants étaient préoccupés par la collecte de renseignements personnels effectuée par Statistique Canada et ont refusé de répondre aux questions du recensement, celles-ci leur paraissant manqué de respect envers leur vie privée.

D'autres ont fait valoir la promesse (ou l'absence) de confidentialité entourant les réponses au recensement. La plainte la plus fréquente à ce sujet était que des voisins ou des connaissances, employés lors du recensement, en recueillaient les résultats. Les plaignants croyaient que leur questionnaire complété serait envoyé directement à Statistique Canada à Ottawa et qu'il serait révisé par un fonctionnaire anonyme, et non par quelqu'un de leur quartier. L'enquête tire maintenant à sa fin et ses résultats seront partagés avec Statistique Canada.

C'est la première fois que notre Bureau entreprend une enquête aussi longue et complexe et cela nous a coûté beaucoup. Les presque six mois qu'y ont consacré trois enquêteurs principaux, ont fait qu'ils n'ont pu se vouer à d'autres tâches. C'est la raison principale qui explique qu'il y ait moins de dossiers complétés que l'an passé. Le roulement dans le personnel (et la formation des nouveaux venus) y ont aussi contribué, augmentant la pile de dossiers non réglés.

Une nouvelle politique au sujet de CIPC

Le Centre d'information de la police canadienne (CIPC) continue d'être la cible de plaintes et de demandes de renseignements concernant la cueillette, l'usage et la communication des renseignements personnels que sa base de données renferme. Le CIPC, constitué de bases de données policières est subventionné par le fédéral et administré par la GRC. Cependant, il est chapeauté par un Comité consultatif constitué des principaux services de polices municipaux et provinciaux, qui contribuent et ont accès aux renseignements.

Plusieurs nous disent qu'ils ne peuvent obtenir leurs renseignements personnels sur le CIPC parce que les services de police ne peuvent pas divulguer des renseignements qui leur ont été fournis par d'autres . Par exemple, la GRC ne peut communiquer des renseignements reçus du service de police d'Ottawa.

Notre bureau a fait part de ses préoccupations face à l'administration du CIPC dans des rapports antérieurs et a recommandé que la GRC consulte les utilisateurs du CIPC afin qu'on introduise un Code de protection volontaire des renseignements personnels dans les bases de données. Ceci contribuerait à instaurer une meilleure protection en ce qui concerne la collecte, l'usage et la communication des renseignements personnels, et permettrait aux individus d'avoir accès à leurs renseignements personnels et de corriger ces informations, s'il y a lieu.

Des félicitations s'imposent. En effet, le CIPC a approuvé et mis en oeuvre un code d'éthique en novembre 1991, code qui rejoint nos préoccupations—particulièrement celles touchant les droits d'accès. Il permet aux individus de demander accès à leurs renseignements personnels contenus dans le CIPC et de demander une correction, lorsque nécessaire.

Les dix premiers

L'an passé, pour la première fois le Commissariat identifiait ses dix plus gros clients—un groupe qui représentait 80 pourcent du total de sa charge de travail. Huit de ces dix ministères font de nouveau la liste cette année : le Service correctionnel du Canada, la Société canadienne des postes, Emploi et Immigration Canada, Revenu Canada (Impôt), la Défense nationale, le Bureau canadien du renseignement de sécurité, la GRC et les Archives nationales.

S'est joint à la liste, la Commission de l'Immigration et du statut de réfugié (CISR) avec 68 plaintes —les premières plaintes concernant la vie privée reçues à l'endroit du CISR. Cependant, 67 de ces plaintes furent déposées par le même plaignant, incluant 33 plaintes de délais considérées bien fondées. Les enquêtes concernant les 33 plaintes d'accès sont en cours.

Plaintes par motifs et résultats

	Résultats				
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Accès	5	102	260	41	408
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Correction/Annotation	0	0	29	0	29
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Langue	0	2	0	0	2
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Collection	1	2	35	4	42
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Usage & Communication	3	9	51	3	66
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Délais	138	3	90	11	242
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
TOTAL	152	117	448	85	782

Une autre hausse importante est survenue à Revenu Canada (Douane et accises). Leurs 72 plaintes représentent une augmentation cinq fois supérieure aux données de l'an passé.

Le rapport de l'an dernier applaudissait les efforts du Service correctionnel du Canada pour circonscrire son problème de non respect des délais. Malheureusement, les plaintes de délais ont triplées cette année—160 (comparé à 50 l'an passé). Ces plaintes représentent 34 pourcent de notre volume de plaintes de non respect des délais. Cependant, ceci nécessite une explication. Le SCC a modifié ses procédures de traitement des renseignements des détenus qu'il reçoit des gouvernemenents municipaux et provinciaux ainsi que des services de police. Le SCC effectuait auparavant automatiquement des dispenses à l'information confidentielle reçues des autres gouvernements. Cependant, après quelques années de pression exercée par notre bureau, le SCC demande maintenant aux organismes d'où proviennent les informations, la permission de les communiquer.

Ceci occasionne des délais pour les demandeurs. Face à l'augmentation de sa charge de travail et la diminution de ses ressources, le SCC doit choisir le moindre mal : donner une réponse incomplète mais en respectant les délais—ou donner des réponses plus satisfaisantes, mais risquer de dépasser les délais prescrits.

D'autres ministères ont aussi de la difficulté à rencontrer les délais : les Archives nationales, Revenu Canada (Impôt) et la Défense nationale.

Vers la fin de l'année fiscale, le bureau a modifié sa façon de comptabiliser les plaintes de délais. Fréquemment, les plaignants remettaient en question les avis de prorogation du délai de 30 jours expédiés par les ministères lorsque ceux-ci voulaient consulter d'autres organisations ou lorsque l'observation du délai entraverait de façon sérieuse le fonctionnement de l'institution. Notre bureau ne comptabilisait pas le nombre de plaintes qui visaient les avis de prorogation du délai. Les plaintes de délais sont maintenant divisées en deux catégories : le non respect du délai et l'avis de prorogation du délai. Cela contribue aussi à identifier les ministères qui continuent de négliger de répondre aux demandes en temps.

Dans des périodes de restrictions budgétaires, il est difficile de prêcher aux ministères la nécessité de respecter les délais. Les budgets et le personnel ont été diminués dans la plupart des ministères et le service au public en souffre.

Quoique le nombre de plaintes de délais et d'accès reçues ont augmenté de 31 pourcent, de 855 l'an passé à 1 118 en 1991-1992— le nombre de plaintes concernant les collectes, les usages et les communications non autorisés de renseignements personnels a chuté de 26 pourcent—de 384 en 1990-1991 à 284 en 1991-1992.

Prestation des institutions fédérales

La GRC continue de se distinguer par le maintien du très grand respect qu'elle accorde pour l'esprit et la lettre de la Loi. Seulement une des plaintes portées contre elle s'est révélée bien fondée, tandis que 40 n'étaient pas fondées et que trois autres ont été abandonnées. Le SCRS doit aussi être félicité : sur les 56 plaintes portées à son endroit, seulement cinq ont été trouvées bien fondées, et elles ont toutes été résolues.

L'an passé le SCC a eu la plus haute proportion de plaintes bien fondées, avec Emploi et Immigration Canada, Revenu Canada (Impôt) et la Défense nationale qui n'étaient pas très loin derrière. Cette année, même s'il continue d'être au premier rang pour le nombre de plaintes reçues (un total de 287), seulement 27 pourcent des plaintes portées à son endroit, se sont avérées bien fondées. Environ la moitié des plaintes portées contre Emploi et Immigration Canada et Revenu Canada (Impôt) et 32 pourcent de celles à l'endroit de la Défense nationale ont été considérées bien fondées.

Le nombre de plaintes abandonnées cette année est élevé. Il se chiffre à 65, ce qui représente 8 pourcent des dossiers qui ont été fermés. Cependant, la majorité ont été abandonnées lorsque les institutions gouvernementales ont été avisé de notre intention d'enquêter, ce qui les à inciter a résoudre le problème. Évidemment, c'est ce en quoi consiste le rôle d'un ombudsman—résoudre des problèmes, non compter des plaintes.

Les dix ministères les plus visés selon les plaintes reçues

		Motifs		
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Service correctionnel du Canada	267	92	160	35
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Emploi et Immigration Canada	135	72	26	37
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Défense nationale	99	20	63	16
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Gendarmerie royale du Canada	84	67	4	13
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Commission de l'immigration et du [illegible]	66	33	33	2
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
AUTRE	273	119	55	99
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Propositions pour de nouveaux fichiers inconsultables

Le Commissariat a été consulté à deux reprises au cours de l'année sur des propositions visant l'établissement de deux nouveaux fichiers inconsultables. La GRC a avisé le Commissaire de son intention de demander l'approbation du Cabinet afin de créer un fichier inconsultable pour ses dossiers d'enquêtes relatives à la sécurité nationale. Le SCRS a également informé le Commissaire relativement à son projet de présenter une demande pour la création d'un fichier inconsultable touchant ses dossiers d'enquêtes.

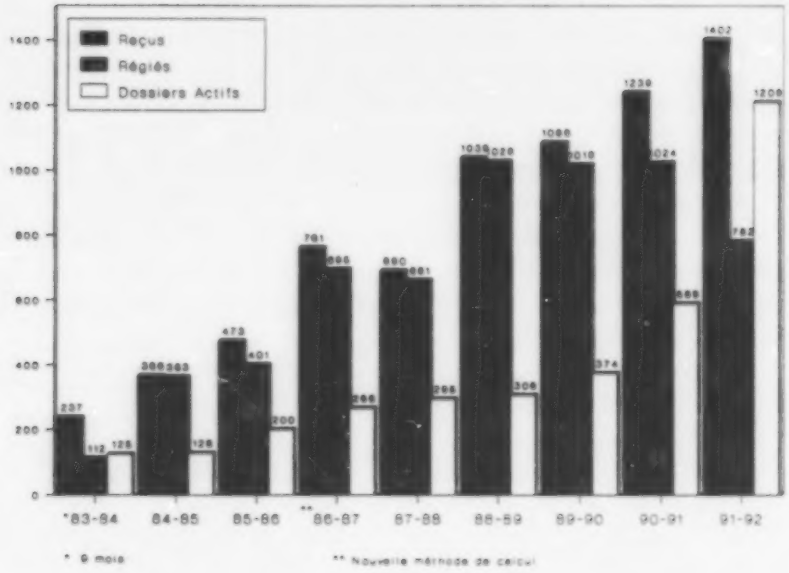
L'examen de ces deux fichiers par le personnel du Commissariat a démontré qu'ils sont constitués principalement de renseignements personnels préparés ou obtenus dans le cadre d'enquêtes criminelles, dont la divulgation risquerait vraisemblablement de porter préjudice à la conduite des affaires internationales du Canada ou à sa défense (articles 21 et 22 de la *Loi sur la protection des renseignements personnels*). Le Commissaire ne désire pas se prononcer sur la validité de ces dispenses afin d'éviter de se placer en situation de conflit d'intérêt au cas où il recevrait une plainte sur des renseignements conservés dans ces fichiers.

Demande pour plus de ressources

Avec une augmentation de 13 pourcent dans le nombre des plaintes reçues au cours de l'exercice, le Commissariat se retrouve avec un arriéré qui correspond à presque une année de travail —1 209 plaintes en souffrance à la fin de l'année. Comme nous l'avions annoncé dans le rapport annuel de l'an dernier, ceci a eu pour effet d'augmenter la charge de travail des enquêteurs à 200 chacun. En conséquence, les clients doivent maintenant s'attendre à des délais plus longs afin d'obtenir la décision du Commissaire sur leurs plaintes.

Le Conseil du Trésor a alloué au Commissariat deux années-personnes additionnelles afin d'augmenter le nombre d'agents à la vie privée. Mais si les plaintes continuent d'arriver au même rythme que l'an passée, le Commissariat se retrouvera avec plus de 2 000 dossiers d'enquêtes ouverts. Une telle situation risque de devenir incontrôlable.

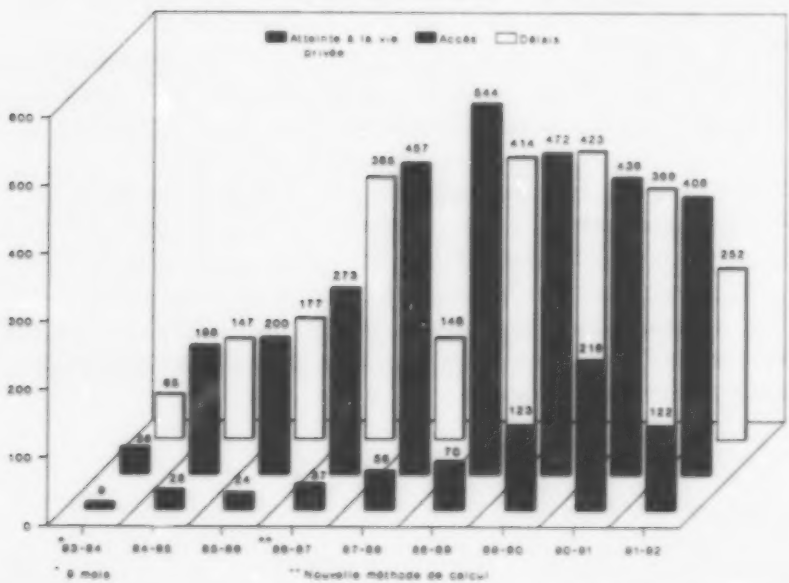
Nombre de dossiers 1983-92



* 9 mois

** Nouvelle méthode de calcul

Plaintes réglées et motifs 1983-92



* 9 mois

** Nouvelle méthode de calcul

Plaintes réglées par motifs 1991-92

Origine des plaintes réglées

Terre-Neuve	5
Île-du-Prince-Édouard	4
Nouvelle-Écosse	43
Nouveau-Brunswick	20
Québec	48
Région de la Capitale nationale - Québec	17
Région de la Capitale nationale - Ontario	114
Ontario	226
Manitoba	28
Saskatchewan	30
Alberta	94
Colombie-Britannique	144
Territoires du Nord-Ouest	4
Yukon	2
Hors Canada	3
TOTAL	782

Plaintes réglées par institutions et résultats

Ministère	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Anciens combattants Canada	7	0	0	7	0
[illegible]	13	0	7	6	0
Affaires indiennes et du Nord Canada	11	7	0	4	0
[illegible]	3	0	2	1	0
Approvisionnements et Services Canada	7	1	0	6	0
[illegible]	10	2	1	8	1
Banque du Canada	2	0	1	1	0
[illegible]	1	0	0	1	0
Bureau du surintendant des institutions financières Canada	3	2	1	0	0
[illegible]	1	0	1	0	0
Commission canadienne des droits de la personne	2	0	0	2	0
[illegible]	1	0	1	0	0
Commission de l'immigration et du statut de réfugié	34	33	0	0	1
[illegible]	1	0	0	1	0
Commission de la Fonction publique du Canada	6	0	3	2	1
[illegible]	1	0	0	1	0
Commission nationale des libérations conditionnelles	36	6	5	23	1
[illegible]	1	0	0	1	0
Conseil de la radiodiffusion et des télécommunications canadiennes	1	0	0	1	0
[illegible]	6	0	0	3	3

Plaintes réglées par institutions et résultats

Ministère	Résultats				
	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Défense nationale	110	25	10	65	10
Emploi et Immigration Canada	71	11	22	30	8
Forêts Canada	1	0	0	1	0
Gendarmerie royale du Canada	44	0	1	40	3
Justice Canada	8	0	1	7	0
Monnaie royale canadienne	1	0	0	1	0
Pêches et Océans	10	1	1	8	0
Revenu Canada, Douanes et Accise	25	15	4	5	1
Revenu Canada, Impôt	67	31	4	31	1
Santé et Bien-être social Canada	7	2	0	5	0
Secrétariat d'État du Canada	2	0	0	1	1
Service canadien du renseignement de sécurité	53	0	5	42	9
Service correctionnel Canada	130	10	25	76	19
Société canadienne des Postes	97	2	9	85	1
Société du crédit agricole Canada	1	0	1	0	0
Solliciteur général Canada	5	0	0	5	0
Statistique Canada	3	0	0	1	2
Transports Canada	20	2	12	6	0
Travail Canada	3	2	0	1	0
Travaux publics Canada	2	0	0	2	0
TOTAL	782	152	117	448	65

Quelques cas

Le CIPC restreint l'identification des personnes souffrant du SIDA

Un groupe d'organismes communautaires de Vancouver a demandé au Commissaire d'enquêter sur des allégations que les bases de données du Centre d'information de la police canadienne (CIPC) identifiaient les personnes porteuses du VIH qui y figuraient.

Même si personne ne pouvait faire état d'un fait précis et s'il n'est pas du tout sûr que le CIPC relève de sa compétence, le Commissaire a décidé de faire enquête officieusement.

La GRC (qui administre le CIPC) a expliqué que les renseignements sur les individus fichés au Centre pouvaient comporter une mention «C» servant à indiquer que l'intéressé souffre d'une maladie contagieuse. Cette mention a pour objet d'aider la police à trouver les personnes ayant des maladies transmissibles qui se sont évadées ou échappées d'hôpitaux ou de pénitenciers. Elle doit aussi aider la police à prévenir les personnes qui auraient pu être exposées aux maladies véhiculées par ces porteurs.

Le comité consultatif du CIPC a demandé une opinion juridique sur l'identification des personnes porteuses du VIH et du SIDA, puis il a modifié sa politique, qui interdit maintenant l'identification des personnes porteuses de ces virus à moins qu'un porteur ait menacé de les transmettre en ayant recours à la violence ou qu'il ait été accusé d'avoir enfreint les lois sur la santé publique en transmettant délibérément les virus.

De plus, le CIPC a communiqué avec tous les organismes qui ont accès à ces bases de données pour leur expliquer sa nouvelle politique. Une vérification ultérieure a relevé 96 mentions «C» (les personnes ne sont pas nécessairement porteuses du VIH ou du SIDA). Depuis, le CIPC a envoyé un rappel aux utilisateurs et fait une autre vérification qui a révélé qu'il ne lui restait plus que 40 fiches portant une mention «C», toutes parfaitement justifiées à des fins policières.

Enfin, un représentant de la GRC est allé rencontrer les membres de la coalition à Vancouver, avec l'enquêteur du Commissariat, pour leur expliquer la situation et pour répondre à leurs questions. La coalition a semblé satisfaite du résultat de l'enquête. Le Commissaire est particulièrement reconnaissant au CIPC et à la GRC de l'ouverture d'esprit avec laquelle les deux organismes ont su écouter les inquiétudes très réelles des organisations intéressées, puis y répondre.

L'intimé devrait avoir accès à tout le dossier

Un plaignant a protesté contre le traitement que la Commission de la Fonction publique (CFP) avait réservé à sa demande de consultation d'un dossier d'enquête sur une affaire de harcèlement. Le Commissariat a constaté que la demande n'avait peut-être pas été traitée de façon conséquente.

Le requérant (qui était l'intimé dans l'affaire de harcèlement) n'avait reçu que les parties du dossier que la CFP considérait comme les renseignements personnels le concernant. L'enquête a révélé que la CFP a différentes façons de traiter les dossiers de harcèlement, en fonction du requérant. Si le requérant est le plaignant, la CFP considère tout le dossier comme un ensemble de renseignements personnels qui le concernent et le lui communique intégralement, hormis les exceptions prévues par la *Loi sur la protection des renseignements personnels*.

Toutefois, si le requérant est quelqu'un d'autre, par exemple un témoin ou l'intimé, la CFP ne lui fournit que les documents qu'elle considère comme des renseignements personnels à son égard.

L'enquêteur du Commissariat s'est dit d'avis que, puisque le requérant était aussi l'accusé de harcèlement, le seul intimé, et que tout le dossier avait trait à l'enquête sur une plainte portée contre lui, la CFP aurait dû le lui communiquer intégralement.

Les autorités de la CFP ont accepté de traiter de la même façon les demandes d'information fondées sur la Loi qui émanent des plaignants et des intimés, dans les cas où ces derniers sont des particuliers plutôt que des ministères ou organismes. Dans ce cas-ci, tous les renseignements figurant au dossier d'enquête de la CFP seront communiqués au plaignant, sous réserve des autres exceptions prévues par la Loi.

Puisqu'on n'avait pas refusé de communiquer à l'intéressé des renseignements personnels le concernant, sa plainte n'était pas bien fondée. Toutefois, elle a amené la CFP à lui communiquer tout le contenu du dossier qui ne pouvait être protégé par une exception, ainsi qu'à modifier sa méthode de traitement des demandes.

Les nouveaux mariés ont droit à un traitement égal

Un fonctionnaire du Centre de sécurité des télécommunications (CST) a informé ses supérieurs qu'il allait se marier, conformément à la procédure que doivent respecter tous les fonctionnaires fédéraux ayant l'autorisation de sécurité «Secret» ou «Très secret». Le fonctionnaire a donc donné le nom, la date de naissance, l'adresse et le nom de l'employeur de sa future épouse, comme l'exige le questionnaire pour l'obtention de l'autorisation de sécurité du gouvernement.

Toutefois, le CST ne s'est pas arrêté là; il a aussi demandé des détails sur le lieu de résidence et l'emploi de l'intéressée au cours des cinq années précédentes. À ce moment-là, celle-ci a porté plainte au Commissaire à la protection de la vie privée : selon elle, en exigeant ces renseignements supplémentaires, le CST portait atteinte à son droit à l'intimité. De plus, il aurait dû lui demander les renseignements en question directement plutôt que de chercher à les obtenir d'un tiers.

L'enquête a révélé que la politique du CST sur les vérifications de fiabilité est différente de celle de la plupart des autres ministères et organismes fédéraux, qui se contentent des renseignements fournis par les fonctionnaires dans le questionnaire qu'ils remplissent pour obtenir leur autorisation de sécurité. Qui plus est, les fonctionnaires nouvellement embauchés par le CST ne sont pas tenus de fournir ces renseignements détaillés sur leur conjoint. Seuls les fonctionnaires titularisés qui changent de situation familiale doivent fournir des détails sur les antécédents, tels lieu de résidence et emploi de leur nouveau conjoint.

Le MDN était le seul ministère fédéral à exiger qu'on lui fournisse ces renseignements supplémentaires dans des circonstances analogues. Il demandait des détails sur le lieu de résidence et l'emploi du conjoint au cours des dix années précédentes.

Il va sans dire qu'on a besoin de détails sur les antécédents personnels des parents des fonctionnaires pour faire des vérifications sur ceux qui sont en mesure d'influencer des gens qui ont accès à des secrets mettant en jeu la sécurité nationale. Toutefois, le Commissariat a du mal à comprendre pourquoi le CST a besoin de plus de renseignements personnels sur les antécédents des nouveaux conjoints de ses employés titularisés que sur que sur les conjoints de ses nouveaux employés.

Les dirigeants du CST ont été persuadés d'harmoniser leurs politiques avec celles des autres ministères. Ironiquement, le MDN avait déjà modifié sa politique en ce sens avant que l'enquête ne soit terminée et que le Commissariat le lui demande.

La plainte, jugée bien fondée, a donc été résolue.

Les réponses de grief ne sont pas destinées à un affichage public

Un employé du ministère de la Défense nationale s'est plaint auprès du Commissaire qu'un surveillant avait affiché une copie de la lettre qui lui avait été adressée en réponse à un grief déposé auprès de son employeur. La lettre comportait son nom, son adresse de même que ses idées et ses opinions personnelles relativement à la politique de fumage et anti- tabagisme du ministère.

L'enquête a révélé qu'une copie de la lettre avait effectivement été affichée sur un babillard dans une salle où travaillait le plaignant, et où d'autres employés civils et militaires pouvaient la voir. Il a été établi que le surveillant avait agi sous les ordres de son supérieur dans le but d'informer le personnel de respecter la politique de fumage et anti-tabagisme du ministère.

À la suite de l'enquête, les représentants du ministère ont reconnu que la lettre en question n'aurait jamais dû servir de rappel aux employés de ne pas fumer dans les édifices de la Défense nationale. Le ministère a confirmé que des mesures correctives avaient été prises afin d'empêcher qu'une situation semblable ne se reproduise.

La plainte, jugée bien fondée, a donc été résolue.

On assomme un maringouin à coups de marteau

Au cours d'une enquête à la suite d'une plainte de harcèlement, Revenu Canada (Douanes et accises) fouille le bureau d'un employé soupçonné d'être l'auteur d'une note anonyme laissée sur le bureau d'un collègue. Les enquêteurs de Revenu Canada ont photocopié son annuaire téléphonique et ont prélevé de son dossier personnel des renseignements personnels afin de les soumettre à une analyse par des experts en écriture.

À la suite de quoi, l'employé s'est plaint au Commissaire à la protection de la vie privée, que Revenu Canada avait divulgué des renseignements personnels sans son autorisation. L'enquête du Commissaire a révélé que des documents personnels avaient été pris et utilisés dans le cadre de l'enquête de harcèlement et que ces renseignements avaient été communiqués à l'extérieur du ministère sans le consentement du plaignant.

Les documents comprenaient l'état de prestations de l'employé — y compris des renseignements médicaux — ainsi que son formulaire de renseignements personnels en entier qui indiquait son niveau de scolarité, les emplois précédents, des références personnelles, de même que les noms des membres de sa famille, les occupations ainsi que les adresses de ces derniers. Le Commissaire a conclu que l'utilisation de ce type de documents personnels au cours d'une enquête interne pouvait difficilement cadrer avec le but de la collecte originale de ceux-ci.

Revenu Canada s'est excusé auprès du plaignant pour avoir communiqué ses renseignements personnels et a modifié son manuel d'enquêtes internes pour s'assurer qu'à l'avenir les enquêteurs n'utiliseront ou ne dévoilent pas ce genre de renseignements personnels sans le consentement de la personne.

Le délateur anonyme n'était pas EIC

Un plaignant a déclaré au Commissaire qu'Emploi et Immigration Canada avait divulgué à son ex-femme des renseignements sur ses revenus tirés de son dossier d'assurance-chômage. Puis, elle s'était servie de ces renseignements pour s'adresser aux tribunaux afin d'obtenir une augmentation de sa pension alimentaire.

L'enquêteur du Commissariat a interrogé les deux employés d'EIC qui s'étaient occupé du plaignant, et ceux-ci ont nié avoir divulgué des renseignements personnels à son sujet à des personnes qui n'avaient pas été autorisées à les avoir. L'ex-femme du plaignant et son conjoint ont aussi été interrogés; ils ont nié avoir obtenu les renseignements d'EIC, en disant qu'ils leur venaient d'un appel anonyme.

Le Commissaire a conclu que rien ne prouvait l'allégation du plaignant que c'étaient des fonctionnaires d'EIC qui étaient à l'origine de la divulgation et a rejeté la plainte.

Le plaignant a révélé lui-même son identité

Un homme a porté plainte au Commissaire en disant que des représentants d'Emploi et Immigration Canada avaient révélé à un centre subventionné par EIC qu'il avait demandé de l'information à son sujet en vertu de la *Loi à l'accès à l'information*. Le plaignant a déclaré à juste titre que l'avoir identifié à l'organisme en question équivalait à une communication abusive de renseignements personnels.

Toutefois, l'enquête a révélé que le plaignant demandait chaque année de l'information sur le centre à EIC - en invoquant la *Loi à l'accès à l'information* -, depuis qu'il s'était querellé avec ses dirigeants. Le personnel du centre le connaissait bien, et il aurait parlé ouvertement de ses demandes d'accès aux dossiers.

Quand la demande est arrivée au Centre, son directeur a tout simplement assumé l'identité du requérant. D'après lui, il ne fallait pas nécessairement être un génie pour cela...

Comme rien ne prouvait qu'EIC avait révélé d'où provenait la demande, le Commissaire a conclu que la plainte n'était pas bien fondée.

Oui, les bandes audio des aveugles peuvent être envoyées sous pli «cacheté»

Un aveugle a porté plainte au Commissaire en disant que la Société canadienne des postes portait atteinte à son droit à l'intimité en exigeant que les aveugles expédient leurs bandes-lettres dans des emballages non cachetés.

L'enquêteur du Commissariat a appris que les aveugles sont autorisés à envoyer leurs bandes-lettres par la poste gratuitement, mais qu'ils doivent les emballer de façon que le personnel de la Société puisse ouvrir facilement l'emballage afin de vérifier si l'envoi est bien conforme aux règlements.

Le plaignant a accepté que l'enquêteur demande l'avis de l'Institut national canadien pour les aveugles (INCA). L'INCA a expliqué que le privilège d'envoi postal gratuit qui lui est accordé équivaut à une subvention de près de trois millions de dollars par année qu'il ne voudrait pas perdre.

La nature même des cassettes audio fait qu'elles ne peuvent pas être mises à la poste comme des lettres ordinaires; les expéditeurs doivent utiliser des enveloppes coussinées spéciales. Pour les livres «parlants» qui constituent la plus grande partie de ses envois, l'INCA a conçu une pochette de plastique réutilisable, fermée par une bande Velcro, qui est pratique et se prête bien aux inspections. Pour ses autres envois, elle utilise de petites enveloppes coussinées fermées avec du ruban gommé ou des agrafes. La Société canadienne des postes ne s'oppose pas à ce mode de fermeture des enveloppes, et le représentant de l'INCA a déclaré à l'enquêteur n'avoir jamais entendu parler d'un aveugle qui aurait eu des problèmes avec des enveloppes fermées de cette façon.

Selon le représentant de l'INCA, le règlement postal stipule que l'enveloppe doit être fermée de façon que son contenu puisse être facilement inspecté. Il n'est pas interdit de la cacheter. D'après lui, le plaignant n'avait qu'à fermer ses enveloppes avec des agrafes pour qu'il soit relativement facile de vérifier si elles avaient été ouvertes.

La Société canadienne des postes illustre sa flexibilité sur la question du privilège d'envoi en citant par exemple le cas d'aveugles qui ont déjà retourné des cassettophones à l'INCA pour les faire réparer et ce sans payer de frais de poste. L'INCA a déclaré que ce genre d'envoi ne devrait manifestement pas être gratuit.

L'enquêteur a expliqué la procédure et la position de l'INCA au plaignant, qui a dit reconnaître que son droit à l'intimité n'avait pas été violé sans raison par la Société canadienne des postes. Le Commissaire a conclu que la plainte n'était pas bien fondée.

La divulgation était une erreur, mais à qui la faute?

Une plainte portée contre la GRC a montré qu'il est parfois impossible d'arriver au fond du problème.

Un homme s'est plaint au Commissaire quand il a appris que la GRC avait envoyé à la Société canadienne des postes un exemplaire de ses empreintes digitales et de son casier judiciaire, sans qu'on le lui ait demandé. Il n'y avait apparemment aucune raison pour que la GRC divulgue le casier judiciaire du plaignant, étant donné qu'on lui avait accordé un pardon. Autrement dit, son casier aurait dû être scellé.

L'enquêteur du Commissariat a été incapable d'obtenir une explication satisfaisante. La vérification n'a pas donné de résultats probants, et le Commissaire a dû rendre sa décision en se fondant sur le peu d'information dont il disposait.

L'enquête a révélé que les Services de sécurité de la Société canadienne des postes avaient reçu de la GRC, au début de 1991, un double du casier judiciaire du plaignant. Bien que ce soit tout à fait normal quand on fait subir une vérification de sécurité aux employés de la Société ou aux candidats qui y postulent un emploi, rien auprès des Services de sécurité n'indiquait qu'on ait demandé ces renseignements. Le plaignant n'était ni un employé, ni un candidat, et les Services de sécurité avaient rangé le double du casier judiciaire dans un dossier provisoire.

À la demande de l'enquêteur, la GRC a examiné ses dossiers, ce qui lui a permis de trouver la note de distribution «Bureau de poste d'Ottawa» à côté de la mention de la condamnation du plaignant. Toutefois, cela n'explique pas pourquoi la GRC avait envoyé un double du casier judiciaire du plaignant à la Société canadienne des postes.

L'enquête s'est poursuivie et le Commissaire a appris que le plaignant avait travaillé brièvement aux Postes il y a plus de dix ans. À l'époque, il avait fait l'objet d'une vérification de fiabilité (pour laquelle on prend les empreintes digitales); c'est ce qui explique l'existence de la note de distribution au bureau de poste. Une fois que le plaignant a quitté cet emploi, son dossier personnel - avec ses empreintes digitales - aurait normalement dû être transféré au Centre national des dossiers du personnel.

Le plaignant est redevenu fonctionnaire fédéral et a récemment fait l'objet d'une vérification périodique de sécurité, pour laquelle la GRC doit consulter son casier judiciaire. Étant donné que personne n'avait retiré la note de distribution figurant sur la vieille liste, le double du casier, mis à jour, a été envoyé à la Société canadienne des postes.

L'explication qui précède est largement fondée sur une reconstruction des événements basée sur des probabilités. Elle n'a rien de définitif. Le Commissaire a conclu que les renseignements avaient été communiqués à tort, mais, faute de détails, il n'était en mesure de blâmer personne.

Toutefois, il a pu rassurer le plaignant en lui disant que la Société canadienne des postes n'a plus ses empreintes digitales ni le double de son casier judiciaire, et que ces renseignements ont été bien protégés pendant le peu de temps qu'elle les a eus en sa possession. De plus, la GRC n'a plus ses empreintes digitales, elle non plus.

Le refus était légal mais inutile

Un homme d'Ottawa a demandé au Commissaire d'enquêter sur plusieurs plaintes qu'il avait portées contre Consommation et Affaires commerciales Canada (CCC), en disant que le ministère avait eu tort de lui refuser l'accès aux renseignements personnels qui le concernent. Le plaignant avait déjà porté plainte en vertu de la *Loi sur la concurrence*. Comme les résultats de l'enquête l'avaient laissé sur sa faim, il voulait avoir accès aux commentaires que le personnel du ministère avait faits à son sujet dans le dossier.

L'enquête du Commissaire a confirmé que Consommation et Affaires commerciales Canada avait refusé de communiquer des renseignements recueillis par son directeur des Enquêtes et Recherches, en disant qu'ils l'avaient été au cours d'une enquête légale. Étant donné que la direction générale en question est l'un des «organismes d'enquête» mentionnés dans la *Loi sur la protection des renseignements personnels*, l'alinéa 22(1)*a)* de la Loi l'autorise à refuser de communiquer les renseignements obtenus au cours de ses enquêtes.

Effectivement, comme les renseignements avaient été recueillis pendant que le directeur des Enquêtes et Recherches instruisait une plainte portée en vertu de la *Loi sur la concurrence*, le ministère avait le droit de refuser de les communiquer. Néanmoins, le Commissaire a déclaré que les renseignements en question étaient relativement anodins, et que le plaignant en connaissait probablement déjà la teneur. Ses arguments et son raisonnement n'ont toutefois pas réussi à convaincre le ministère de communiquer les renseignements demandés. Le ministère a tenu à se prévaloir de son droit de refuser, même s'il était fort peu probable qu'il aurait nui à son enquête ou à qui que ce soit en communiquant les renseignements demandés au plaignant.

Étant donné que Consommation et Affaires commerciales Canada n'est pas tenu de démontrer qu'il y a un risque à communiquer les renseignements demandés, en vertu de l'alinéa 22(1)*a)*, le Commissaire a été bien obligé de dire au plaignant que, même s'il n'était pas du tout d'accord avec le ministère sur ce point, celui-ci avait respecté la lettre de la loi. Autrement dit, il devait juger que la plainte n'était pas bien fondée.

Les dossiers de la Commission des accidents du travail de l'Ontario ne sont plus «confidentiels»

Un avocat s'est plaint que Santé et Bien-être social Canada avait refusé de lui donner accès à 20 pages du dossier médical d'invalidité du Régime de pensions du Canada de son client, dossier provenant de la Commission des accidents du travail de l'Ontario.

À la suggestion de Santé et Bien-être social, l'avocat s'est adressé directement à la Commission, qui lui a envoyé plus de documents que le ministère ne lui en avait refusés, ce qui l'a laissé dans l'impossibilité de juger sur quels documents le ministère s'était fondé pour rejeter la demande de son client. L'avocat a déclaré qu'il lui serait impossible de représenter convenablement son client dans une procédure d'appel de pension s'il ne savait pas exactement quels documents le ministère avait reçus de la Commission.

L'enquêteur a constaté que Santé et Bien-être social avait refusé de communiquer 20 pages à l'avocat en invoquant l'alinéa 19(1)*c)* de la *Loi sur la protection des renseignements personnels*, qui enjoint aux institutions fédérales de refuser de communiquer des renseignements personnels qu'elles ont obtenus «à titre confidentiel» des gouvernements des provinces ou de leurs organismes. Il n'y a aucune possibilité d'interprétation et aucune latitude aux organismes fédéraux à cet égard.

Par conséquent, une fois qu'un gouvernement provincial ou une administration municipale déclare que des renseignements sont confidentiels, il est interdit aux organismes fédéraux de les divulguer, si banals soient-ils.

L'enquête a confirmé que, depuis le 14 décembre 1983, il est convenu que tous les renseignements communiqués à Santé et Bien-être social par la Commission des accidents du travail de l'Ontario sont confidentiels et ne doivent pas être divulgués, sauf par la Commission elle-même.

Nonobstant cette entente, l'enquêteur du Commissariat a demandé à Santé et Bien-être social de demander à la direction de la Commission l'autorisation de communiquer les renseignements en question. Le ministère a bien voulu le faire, à la suite de quoi la Commission a modifié sa politique l'autorisant à communiquer les renseignements directement aux personnes qui en font la demande.

C'est un changement important de la politique qui devrait simplifier la procédure nécessaire pour bien des requérants.

Le Commissaire a conclu que la plainte n'était pas bien fondée, étant donné que Santé et Bien-être social n'avait pas auparavant le droit de divulguer les renseignements obtenus de la Commission. Il a applaudi à la décision de la Commission de modifier sa politique.

Aviser le Commissaire

Cette année, le Commissariat a reçu 43 préavis d'organismes gouvernementaux qui comptaient divulguer des renseignements personnels pour des raisons «d'intérêt public» ou à l'avantage de l'individu concerné. Dans ce contexte, le rôle du Commissaire se borne à informer les intéressés de la divulgation envisagée, s'il le juge bon. Il peut conseiller de ne pas divulguer les renseignements, mais il ne peut pas interdire de le faire.

Le personnel du Commissariat dépouille les préavis, de façon à ce que le Commissaire puisse étudier les plaintes qu'il pourrait recevoir à ce sujet sans avoir déjà jugé de l'opportunité de la divulgation.

L'alinéa 8(2)*m)* de la Loi est censé porter sur les divulgations de nature exceptionnelle, et pourtant, bien des préavis sont devenus si répétitifs qu'ils imposent une lourde charge administrative tant au ministère responsable qu'au Commissariat lui-même.

Par exemple, Multiculturalisme et Citoyenneté Canada envoie régulièrement un préavis de divulgation au Commissaire avant de confirmer le statut de citoyen canadien des personnes sélectionnées pour être nommées à l'Ordre du Canada. Étant donné qu'il s'agit là d'une utilisation courante de documents relatifs à la citoyenneté, le Commissariat a proposé au ministère de le faire savoir publiquement et de modifier en conséquence son inscription dans *Info Source*. Le ministère a retenu cette proposition, qui lui a permis d'éliminer de la paperasse dans ses opérations et de donner au public une idée plus claire de la façon dont les renseignements concernant la citoyenneté peuvent être utilisés.

Divulgations du Service correctionnel du Canada - Reprise

L'an dernier, le Commissaire a souligné dans son rapport toute la difficulté de concilier la protection de la vie privée et l'intérêt public, dans le cas de la divulgation de rapports portant sur des évasions de prison au cours desquelles trois personnes avaient été assassinées (voir Rapport annuel 1990-1991).

Le Solliciteur général avait alors refusé de donner au Comité permanent de la Justice et du Solliciteur général les versions intégrales de ces rapports d'enquête, en déclarant que la *Loi sur la protection des renseignements personnels* en interdisait la divulgation.

Son refus avait fait l'objet d'une question de privilège à la Chambre des communes, et le Commissaire par intérim avait été appelé à témoigner devant le Comité permanent des privilèges et des élections, où il avait dit ne voir aucune difficulté à ce que le Solliciteur général communique la version intégrale des rapports au Comité, dans une séance à *huit clos*.

Le Comité des privilèges et des élections a conclu dans son rapport, "qu'aucune disposition de la *Loi sur la protection des renseignements personnels* n'empêche la Chambre des commnes d'adopter un ordre exigeant la production des versions non expurgées des deux rapports. Par conséquent, nous ne croyons pas qu'il soit nécessaire ou souhaitable de modifier la *Loi sur la protection des renseignements personnels* afin de permettre la production de ces rapports".

Le rapport suggérait que des copies des rapports soient mises à la disposition du Comité de la Justice et du Solliciteur général à l'occasion d'une séance à *huit clos*. Voici des exemples d'autres préavis reçus pour des raisons d'intérêt public.

La divulgation entraîne le dépôt d'une plainte au Commissaire

Le Bureau du Conseil privé (BCP) a avisé le Commissaire de son intention de divulguer des renseignements personnels concernant plusieurs personnes à un organisme professionnel qui enquêtait sur la conduite de deux de ses membres. Les documents avaient été déposés en preuve devant une commission fédérale d'enquête.

Le BCP avait obtenu le consentement d'un individu (qui n'était pas visé par une enquête), mais il ne jugeait pas pratique d'obtenir le consentement de tous les intéressés. Le Commissariat s'est dit d'avis que tous ces gens devaient être informés de la divulgation imminente des renseignements, en laissant entendre que l'avis risquerait moins de les perturber s'il émanait directement du BCP. Celui-ci a retenu la proposition et écrit à chacun des intéressés, en exposant les motifs de la divulgation et en citant la disposition pertinente de la *Loi sur la protection des renseignements personnels*.

L'une des personnes en cause s'est opposée à la divulgation et a depuis porté plainte auprès du Commissaire à la protection de la vie privée.

Divulgations en vue de la remise d'une distinction pour bravoure

La GRC a avisé le Commissaire que la Direction des distinctions honorifiques de la Chancellerie (l'une des composantes du Bureau du Gouverneur général) lui avait demandé des renseignements sur l'une des victimes de l'écrasement d'un avion dans l'Arctique en 1972. La Chancellerie envisageait de décerner une distinction pour bravoure (à titre posthume) à un jeune Inuit qui avait survécu à l'écrasement et sauvé la vie du pilote blessé, mais qui était mort avant que les secours arrivent.

La Chancellerie remettait en question toute sa démarche par suite de la publication d'un deuxième livre sur l'accident dans lequel figuraient des détails sur le rôle joué par le jeune homme dans la survie du pilote.

L'enquêteur du Commissariat a étudié les documents que la GRC se proposait de divulguer et il a constaté qu'ils contenaient moins de renseignements personnels que la transcription de l'enquête du coroner ou que l'un ou l'autre des deux livres publiés sur l'écrasement de l'avion. Par ailleurs, les documents qui auraient été divulgués confirmaient l'exactitude de certains des détails du livre en question.

Le Commissariat ne s'est pas opposé à la divulgation, en concluant qu'on n'avait pas besoin d'en informer le seul survivant puisque les renseignements étaient déjà publics.

Une liste de pilotes et de mécaniciens n'a pas été divulguée

Le ministère de la Défense nationale (MDN) a demandé à Transports Canada de lui communiquer une liste de pilotes d'hélicoptères et de mécaniciens d'entretien de la région d'Ottawa, pour pouvoir les informer des possibilités d'emploi à la Défense.

Le Commissariat est rarement favorable à ce genre de divulgation d'une liste générale quand il y a d'autres moyens de communiquer avec les intéressés. La divulgation de la liste est peut-être à l'avantage que ceux qui décrochent des emplois, mais pas à celui des autres, en l'occurrence plusieurs centaines de personnes. Le Commissariat a donc proposé que Transports Canada envoie par la poste des avis pour le MDN, ou que le MDN place tout simplement des annonces dans les journaux locaux et dans les publications professionnelles.

Transports Canada a décidé de ne pas fournir la liste.

Divulgation d'un rapport d'autopsie à un médecin de famille

Un médecin a demandé au ministère de la Défense nationale de lui envoyer le rapport d'autopsie d'un membre des Forces canadiennes qui était mort subitement en faisant du jogging. Le médecin traitait un membre de la famille du militaire décédé et voulait savoir si l'officier souffrait de la même affection susceptible de contribuer à causer une crise cardiaque. Puisqu'on soupçonne que l'affection en question est héréditaire, le médecin voulait commencer immédiatement à traiter les autres membres de la famille du défunt.

Le MDN a communiqué le rapport d'autopsie au médecin, puis il en a informé le Commissaire. Normalement, le Commissariat préfère recevoir un préavis, mais le MDN avait reçu la demande de divulgation pendant la grève de la Fonction publique; il était alors sans personnel de bureau. Le Commissaire ne s'est pas opposé à la divulgation.

Liste d'anciens combattants de la guerre de Corée envoyée à Rideau Hall

Le Bureau du Gouverneur général a été la source d'une autre demande de renseignements personnels, au sujet cette fois d'anciens combattants de la guerre de Corée. L'affaire montre bien à quel point les malentendus sont faciles, lorsqu'or communique par téléphone.

La Chancellerie avait demandé à Anciens combattants Canada de lui donner accès à sa base de données de renseignements personnels sur les anciens combattants admissibles à la Médaille canadienne de service volontaire pour la Corée. La Chancellerie avait besoin de ces renseignements (noms et adresses, langue, numéro de service et confirmation d'admissibilité) pour pouvoir traiter plus vite les demandes d'obtention de cette nouvelle médaille de la guerre de Corée. Le Bureau du Gouverneur général voulait décerner les médailles en novembre 1991.

Anciens combattants Canada a téléphoné au Commissariat au sujet de la demande. À la fin de la conversation, le ministère avait l'impression qu'il lui faudrait obtenir le consentement écrit de chacun des anciens combattants visés. (En fait, ce n'était là qu'une des avenues proposées par le Commissariat.) Ce message a été communiqué au personnel de la Chancellerie qui, dans un réflexe de frustration bien compréhensible, a téléphoné directement au Commissariat.

Le Commissariat a demandé à voir un avis écrit et un échantillon des renseignements que la Chancellerie voulait faire tirer de la base de données. L'examen de ces documents lui a permis de constater que toutes les personnes dont les noms figuraient sur la liste avaient manifesté de l'intérêt pour la médaille, de sorte que la divulgation des renseignements qui les concernaient allait être à leur avantage. D'autre part, le Commissariat a proposé à Anciens combattants Canada de demander à la Chancellerie de s'engager par écrit à n'utiliser les données que dans ce contexte, puis à les détruire ou à les lui retourner.

Le malentendu a vite été réglé et le Gouverneur général a décerné la première des médailles lors d'une cérémonie à Ottawa le 10 novembre 1991.

Une fausse déclaration de citoyenneté canadienne

Le ministère des Affaires extérieures a avisé le Commissaire de son intention d'informer le gouvernement d'un pays étranger qu'un individu arrêté sur le territoire de ce pays pour une affaire de drogue n'était pas citoyen du Canada, même s'il était porteur d'un passeport canadien.

Le gouvernement du pays en question avait saisi le passeport et l'avait remis aux représentants des Affaires extérieures en partant du principe que, si le prévenu était bel et bien citoyen canadien, le Canada allait lui délivrer des documents de voyage à sa libération. Bien entendu, l'ambassade du Canada n'allait pas fournir de services consulaires ou des documents de voyage à un individu qui n'est pas Canadien.

Le Commissariat a reconnu que la divulgation était fondée, étant donné qu'il est d'intérêt public de protéger l'intégrité des passeports canadiens. En outre, il est important que les Canadiens ne soient pas alarmés par des rumeurs sur le refus de services consulaires à de prétendus «citoyens» du Canada.

Demandes de renseignements - Le public réagit

Les agents du Commissariat continuent à répondre à un nombre sans cesse croissant de lettres et d'appels téléphoniques : le Commissariat en a reçu 4 671 au cours de l'année écoulée. La ligne téléphonique (qu'il partage avec le Commissariat à l'information) permet aux Canadiens de l'appeler sans frais de tous les coins du pays et est le seul service national du genre d'accès à l'information et de protection de la vie privée.

Les Canadiens sont de plus en plus au courant des mesures existantes de protection de leur vie privée ainsi que des nouvelles lois ou dispositions législatives envisagées par les gouvernements provinciaux et par les autorités municipales. La Saskatchewan vient tout juste de proclamer sa loi (*Freedom of Information and Privacy Act*) et la Colombie-Britannique et l'Alberta ont toutes deux promis d'adopter des lois analogues dans leurs derniers discours du Trône.

Il reste que les correspondants du Commissariat sont toujours étonnés de constater l'absence totale de réglementation dans le secteur privé. Les nombreux appels de personnes qui ont des difficultés à consulter ou à protéger les renseignements personnels qui les concernent et que détiennent des organisations privées en témoignent. Il est frustrant pour le Commissariat de devoir avouer qu'il n'y peut rien, puisque sa compétence se limite à l'administration fédérale. Pire encore, il est incapable de proposer à ses correspondants des moyens de régler leurs problèmes.

Bien que la *Loi sur la protection des renseignements personnels* soit une loi fédérale, des centaines d'organismes et d'entreprises réglementées par l'administration fédérale lui échappent, notamment les Chemins de fer nationaux du Canada, Via Rail, Air Canada, Énergie atomique du Canada Limitée, diverses corporations de ports, ainsi que des compagnies de téléphone et des institutions financières comme les banques et les compagnies d'assurance.

Le Commissariat a aussi répondu à des appels sur la façon de traiter les renseignements personnels dans les bureaux des députés ainsi qu'à la Commission royale sur les nouvelles techniques de reproduction. Les employés et les clients sont effarés d'apprendre que nous ne pouvons pas intervenir et qu'ils ne peuvent pas non plus invoquer les lois provinciales ou les règlements municipaux.

Les agents du Commissariat chargés des demandes de renseignements passent une grande partie de leur temps à expliquer les mesures limitées de contrôle de l'utilisation des numéros d'assurance sociale (NAS). La plupart des gens croient que l'utilisation du NAS a été limitée par la législation qui a créé les régimes d'assurance-chômage et de pensions, dans les années soixante. Or, en dépit des promesses qui avaient été faites à l'époque, ce n'est pas le cas. Un grand nombre de nos correspondants ont du mal à accepter l'idée que seul le gouvernement fédéral limite son utilisation du NAS.

Trop souvent hélas, les gens doivent choisir entre la protection de leur NAS et l'obtention des biens et des services qu'ils veulent. Vu que le mandat du Commissariat est limité, le personnel encourage maintenant les correspondants à écrire à leurs députés, dans l'espoir que, si plus de députés reçoivent des plaintes, ils pourraient être incités à agir pour contrôler les utilisations abusives du NAS.

Et pourtant, tout n'est pas perdu. Plusieurs organisations s'intéressent à cette question. Au cours de la dernière année, le Commissariat a envoyé de la documentation à la Municipalité régionale de Waterloo, au ministère du Revenu de l'Ontario, aux universités de la Saskatchewan et du Québec, à Nova Corporation et à Maritime Telegraph & Telephone.

En outre, la Commission québécoise d'accès à l'information et de protection de la vie privée mérite des éloges pour ses enquêtes sur les utilisations abusives du NAS dans les organismes gouvernementaux du Québec. Contrairement à la plupart des provinces qui éludent la question parce que le NAS est un numéro d'identification fédéral, la Commission québécoise a saisi l'initiative et elle est intervenue en vertu de sa propre loi sur l'accès à l'information et sur la protection de la vie privée. Résultat? Le Québec n'exige plus qu'on produise son NAS pour obtenir un permis de pêche dans les zones de compétence provinciale. De même, l'industrie de l'assurance-automobile a consenti tacitement à ne plus obliger ses clients à lui fournir leur NAS.

Loin de s'arrêter là, la Commission québécoise enquête actuellement sur d'autres utilisations provinciales du NAS :

- le droit d'Hydro-Québec d'utiliser le NAS pour identifier tant ses employés que ses abonnés;
- la pratique de l'Université Laval d'exiger le NAS de ses étudiants; et
- l'utilisation du NAS par les hôpitaux, notamment pour malades chroniques, les maisons de convalescence et les organismes de logement.

Oui, il est vraiment encourageant de constater que les efforts du gouvernement fédéral ont eu une certaine influence au-delà de son propre secteur de compétence.

Cela dit, en dépit des efforts que le Commissariat a déployés pour clarifier son inscription dans les pages bleues (organismes gouvernementaux) des bottins téléphoniques, plus de la moitié des appels qu'il reçoit sur sa ligne 800 accessible de tous les coins du pays n'ont rien à voir avec l'accès à l'information ou la protection des renseignements personnels. La réceptionniste a dû aiguiller 9 343 correspondants vers Référence Canada, le service central d'information de l'administration fédérale. Le Commissariat tentera une fois de plus de remédier à ce problème maintenant que Bell Canada et les services gouvernementaux responsables du téléphone se donnent la main pour améliorer les pages bleues.

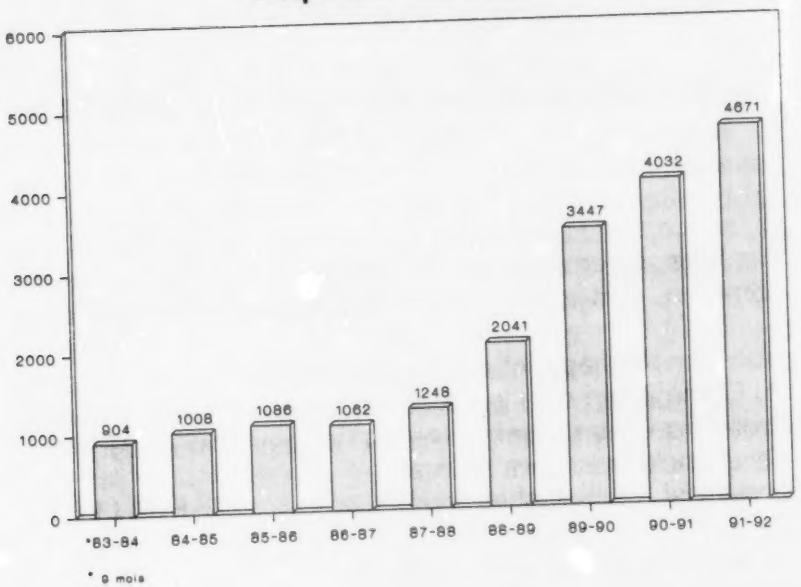
Enfin, le Commissariat a installé cette année un dispositif de communication pour les correspondants souffrant de troubles de l'ouïe et de la parole (ATS).

Les deux tableaux suivants illustrent les statistiques des demandes de renseignements. Le premier compare les nombres de demandes avec ceux des années précédentes; le second est une ventilation par sujet des demandes de l'année écoulée.

DEMANDES DE RENSEIGNEMENTS REÇUES 1991-1992

Qu'est-ce que la Loi sur la protection des renseignements personnels et comment puis-je m'en prévaloir?	2 420 (52 %)
Questions échappant à la compétence du Commissariat/à la Loi sur la protection des renseignements personnels (secteurs fédéral, provincial, municipal et privé)	808 (17 %)
Utilisation justifiée ou abusive du numéro d'assurance sociale (NAS)	588 (13 %)
Demandes au mauvais organisme et questions n'ayant rien à voir avec la Loi sur la protection des renseignements personnels	855 (18 %)
TOTAL	4 671

Requêtes 1983-92



Direction de l'observation

La Direction avait deux objectifs en 1991-1992. Le premier consistait à concentrer ses travaux de vérification sur un organisme national complexe, la Société canadienne d'hypothèques et de logement (SCHL), qui a d'importants volets de traitement électronique des données et de communications. La vérification des activités de la SCHL a donné au personnel l'occasion d'étudier le traitement des données distribuées et les questions de communications électroniques, ainsi que de perfectionner sa méthode de vérification du TED.

Le deuxième objectif de la Direction consistait à faire des vérifications dans plusieurs petits organismes du secteur des droits des femmes et des minorités. La plupart de ces organismes ont d'importantes collections de renseignements personnels, souvent parce qu'ils instruisent des plaintes. Ceux qui ont fait l'objet d'une vérification au cours de la dernière année sont Condition féminine Canada, le Conseil consultatif canadien sur la situation de la femme, la Commission canadienne des droits de la personne et la Commission de l'immigration et du statut de réfugié.

Le personnel de la Direction a aussi terminé ses travaux de vérification au ministère de la Défense nationale, à la Commission de la Capitale nationale, à la Société d'expansion de l'industrie cinématographique canadienne, au Conseil canadien des normes et à diverses commissions de pilotage. Les travaux de vérification entrepris dans treize autres organismes se prolongeront en 1992-1993. Le personnel a aussi

- enquêté sur cinq cas de fichiers perdus ou volés;
- effectué la vérification de trois couplages de données existants à Emploi et Immigration Canada; et
- réalisé un sondage à l'échelle de toute l'administration fédérale sur l'utilisation des évaluations vers le haut (inversées) dans les institutions fédérales.

Tendances et problèmes

Les vérifications réalisées au cours de la dernière année ont révélé des tendances qu'il ne faudrait pas négliger sur la façon de traiter l'information dans l'administration fédérale. La plus manifeste de ces tendances est sans doute le recours croissant de la Fonction publique à des entreprises privées de services et notamment de traitement des renseignements personnels.

Contrats accordés à l'extérieur - qui surveille?

Les contraintes budgétaires imposées aux organismes gouvernementaux en ont incité beaucoup à chercher dans l'entreprise privée certains services naguère internes. Par exemple, des services comme les Programmes d'aide aux employés, la gestion des listes de paye et les vérifications de crédit - avec les renseignements personnels nécessaires dans chaque cas - sont maintenant fréquemment confiés à contrat à des entreprises privées.

Le Commissariat n'a aucune objection à ce que des entreprises privées offrent des services à l'administration fédérale; toutefois, contrairement à celle-ci, ces entreprises ne sont pas assujetties à la *Loi sur la protection des renseignements personnels*. Par conséquent, les dossiers personnels transférés à l'entreprise privée ne bénéficient plus de la moindre protection légale des renseignements qu'ils recèlent, à moins que les contrats passés entre les organismes gouvernementaux et les fournisseurs ne contiennent de clauses expresses à ce sujet. Étant donné que certains ministères et organismes utilisent les formulaires de contrat normalisés d'Approvisionnements et Services Canada alors que d'autres préfèrent les leurs, le manque d'uniformité est la règle plutôt que l'exception. Presque tous les contrats analysés présentaient des lacunes.

Ces lacunes sont les suivantes :

- la propriété des renseignements n'est pas définie;
- l'accès des employés aux dossiers n'est pas assuré;
- l'utilisation ultérieure des renseignements personnels n'est pas limitée;
- il n'y a aucune protection contre la communication non autorisée des renseignements;
- il n'y a pas de dispositions propres à assurer le retrait des dossiers conformément aux règles à l'expiration du contrat;

- les critères de conservation et de retrait ne sont pas précisés; et
- rien n'est prévu pour assurer la capacité du ministère (ou de l'organisme) à vérifier si les règles sont respectées.

Le Commissariat collabore actuellement avec Approvisionnements et Services Canada et avec le Conseil du Trésor en vue de rédiger un contrat normalisé qui devrait remédier à presque tous ces problèmes.

Vérification de la cote de crédit des employés

Les vérificateurs du Commissariat ont aussi constaté des problèmes de surcollecte de renseignements au cours de leur examen des dossiers du personnel. En effet, tous les fonctionnaires nommés pour une période indéterminée - et une grande partie de ceux qui sont mutés ou promus - doivent faire l'objet d'une vérification dite de fiabilité. Le ministère ou l'organisme employeur obtient leur autorisation de vérifier leur cote de crédit auprès des bureaux de crédit locaux. Les cotes de crédit sont une combinaison de lettres et de chiffres qui décrivent l'endettement relatif de l'intéressé et son comportement de débiteur.

Le personnel du Commissariat a relevé là une grande partie des problèmes constatés dans le cas des contrats, mais, dans le cas des vérifications de crédit, il y en a d'autres. Par exemple, les ministères et organismes ayant un effectif important, comme la GRC, la SCHL et le MDN, sont souvent reliés en direct aux ordinateurs des bureaux de crédit, ce qui leur permet d'en tirer nettement plus de données financières personnelles que s'ils demandaient une simple cote de crédit. Les risques d'abus sont évidents, et rien n'empêche les institutions fédérales de chercher à obtenir des renseignements qui ne les concernent pas.

En fait, la plupart des institutions qui ont fait l'objet d'une vérification par le Commissariat tendent à recueillir beaucoup plus de renseignements financiers qu'elles n'en ont besoin. Les enquêteurs ont trouvé dans les dossiers des détails tels que des marges de crédit et des soldes bancaires, là où, une simple cote de crédit aurait suffit. De plus, certains rapports de crédit contenaient des renseignements non seulement sur le fonctionnaire visé, mais aussi sur son conjoint ou sa conjointe. Les bureaux de crédit établissent souvent un relevé des antécédents professionnels et de la cote de crédit du conjoint ou de la conjointe et les annexent aux renseignements concernant l'intéressé, en se servant des numéros d'assurance sociale et des dates de naissance.

Pire, une fois que l'institution gouvernementale a ces renseignements sur le crédit, il arrive souvent qu'elle ne les protège pas convenablement. Dans certains cas, le personnel du Commissariat a constaté que l'on avait télécopié ces renseignements. Dans d'autres cas, ils avaient été stockés dans des disques rigides d'ordinateurs de bureaux, sans protection suffisante.

Enfin, une grande partie des renseignements sur le crédit des fonctionnaires ne sont pas fiables. Des études réalisées par des chercheurs indépendants ont révélé un pourcentage d'erreur élevé dans les dossiers de crédit. Les mises à jour et les corrections sont faites lentement... quand elles le sont. C'est toujours l'intéressé qui doit voir à ce que l'information soit exacte, même si ce sont les magasins et les banques qui la transmettent aux bureaux de crédit.

Transmission électronique des renseignements personnels

Les vérifications ont révélé que les institutions gouvernementales se servent régulièrement de télécopieurs pour envoyer ou recevoir des renseignements personnels. Les transmissions peuvent être interceptées, ou transmises au mauvais numéro. C'est ainsi qu'un fonctionnaire travaillant au Centre d'emploi du Canada à Sarnia, en Ontario, a envoyé des demandes de renseignements sur l'assurance-chômage de quatre personnes au journal local plutôt qu'au bureau d'EIC de London. Il avait appuyé par erreur sur la mauvaise touche de composition rapide, qui correspondait au numéro du journal.

Cette erreur humaine est un bon exemple des conséquences de la transmission de renseignements personnels par télécopieur. Malheureusement, les vérificateurs ont constaté l'existence de cette pratique dans presque toutes les institutions visitées. Dans ce domaine, les politiques et procédures n'évoluent pas au rythme de la technologie. On se pose très peu de question sur le genre d'information dont on devrait autoriser ou interdire la transmission par télécopieur. Bref, les fonctionnaires transmettent toutes sortes de renseignements personnels, des plus banals (listes de participants à des réunions) aux plus délicats (dossiers médicaux et vérifications de crédit).

Le même raisonnement s'applique aux nouveaux systèmes de courrier électronique, qui sont de plus en plus répandus. Les programmes de courrier électronique conçus à cette fin permettent aux utilisateurs des réseaux d'ordinateurs de communiquer et de transférer des données partout dans les réseaux auxquels ils sont reliés. Pourtant, dans ce contexte, il n'existe à peu près pas de politiques ou de procédures servant à assurer la protection des données ou à faire en sorte qu'elles ne soient communiquées qu'à ceux qui ont besoin de savoir.

Qui surveille l'ordinateur?

Une tendance inquiétante se dessine : l'administration gouvernementale ne semble pas avoir les mêmes normes de gestion et de contrôle pour ses fichiers informatiques que pour ses dossiers sur papier. De grandes institutions gouvernementales complexes donnent l'impression de ne pas savoir de quels matériels elles disposent et quels logiciels elles emploient, et encore moins avoir une idée de ceux qui ont accès à leurs systèmes informatiques et de la façon dont ils sont utilisés. Des collections de plus en plus importantes de fichiers de données personnelles sont automatisées, mais les contrôles nécessaires manquent. Dans le cas de données informatisées, parce que celles-ci n'occupent pas un espace défini, on a tendance à en négliger la sécurité.

Ordinateurs portatif : l'administration fédérale s'est automatisée en même temps qu'on miniaturisait l'ordinateur. Aujourd'hui, des appareils au moins aussi puissants que ceux qui occupaient naguère toute une pièce sont de la taille d'un bloc-notes et tiennent facilement dans un porte-documents. Et ce n'est pas fini : la technologie des puces à circuits intégrés est déjà à l'essai, et elle a rendu possible les cartes à mémoire en plastique, c'est-à-dire de minuscules ordinateurs capables de mémoriser et de traiter des données.

Les ordinateurs personnels perfectionnés nécessitent toutefois de nouveaux systèmes de gestion et de contrôle, car les utilisateurs oublient souvent qu'ils sont bien plus que des machines à écrire miniatures. En effet, comme l'ordinateur se souvient de ce qu'il a traité, lorsqu'il est perdu ou volé, tous les renseignements qu'il contient disparaissent avec lui.

Cette année, le Commissariat a dû enquêter sur le vol d'un ordinateur personnel dans les bureaux de Montréal du ministère des Anciens combattants. L'incident témoigne bien de toute la gravité d'une perte comme celle-là. L'ordinateur était utilisé pour les essais d'un nouveau système; on y avait stocké des données sur les pierres tombales de toute la clientèle régionale, soit quelque 20 000 personnes. Heureusement, les renseignements personnels en question étaient très limités, de sorte que le Commissaire a décidé de ne pas informer les intéressés du vol.

L'enquête a révélé que le personnel des Anciens combattants n'avait pas respecté la procédure ministérielle de protection des biens de valeur. Mais il y a pire. Les enquêteurs ont constaté que le ministère n'avait pas de politique ou de procédure sur la conservation et la protection des renseignements personnels stockés sur ordinateur. Le Commissaire a donc recommandé aux Anciens combattants de se donner la politique voulue et d'envisager de stocker les renseignements personnels seulement sur des disquettes pouvant être retirées des ordinateurs et conservées à part. Il a aussi proposé une solution de rechange, le codage des renseignements personnels conservés sur ordinateur pour les rendre inaccessibles aux utilisateurs n'ayant pas les autorisations nécessaires.

Contrôle de l'accès aux réseaux : La combinaison des micro-ordinateurs dans des réseaux locaux ou de plus grande envergure encore représente un nouveau défi pour la protection de la vie privée, celui de déterminer quels utilisateurs devraient avoir accès à quels renseignements. Les vérificateurs du Commissariat constatent souvent que les utilisateurs autorisés des systèmes peuvent fréquemment avoir accès à des renseignements dont ils n'ont pas besoin. Même si les locaux et le matériel informatique sont protégés contre des interventions de l'extérieur, une fois en communication avec le système, les utilisateurs peuvent avoir accès à toutes les données. Il faut qu'on mette au point des systèmes permettant d'empêcher les utilisateurs d'avoir accès à d'autres renseignements que ceux dont ils ont besoin.

Élimination du syndrome de l'écureuil : Les vérificateurs ont constaté qu'il y a très peu de protocoles sur la durée de conservation et le calendrier de retrait des fichiers informatiques, et que, lorsqu'il y en a, les délais sont rarement les mêmes que ceux qui sont prévus pour les dossiers sur papier. L'administration gouvernementale détruit peut-être ses documents de papier, mais une grande partie sont générés électroniquement et reproduits sur des disques rigides ou des disquettes qui semblent être conservés indéfiniment. Par conséquent, les organismes gouvernementaux chargés de conserver et de retirer les dossiers personnels ont intérêt à ne pas négliger non plus leurs versions électroniques.

Description des renseignements détenus par l'administration fédérale

La description qu'*Info Source* donne des renseignements détenus par l'administration fédérale continue à préoccuper le Commissaire. Il est possible que le manque de ressources ait contribué à la situation, mais il n'empêche que les vérificateurs du Commissariat ont bien dû constater qu'*Info Source* est un répertoire incomplet - et parfois inexact - des renseignements personnels détenus par les institutions gouvernementales. Certains ministères ne semblent pas comprendre clairement ce qu'ils devraient inscrire au répertoire, ou comment changer leurs inscriptions.

Par exemple, les ministères et organismes oublient souvent de mentionner dans le répertoire des banques de données aussi communes sur les fonctionnaires fédéraux que les registres des congés et des présences, ceux des voyages et des réinstallations et enfin ceux des cours de formation et de perfectionnement. Parfois, c'est l'inverse qui se passe : les banques de données figurent au répertoire, alors que l'institution ne détient aucun renseignement correspondant; en fait, les banques sont vides. Enfin, il arrive parfois, au gré des vérifications et des enquêtes sur les plaintes, qu'on découvre des renseignements ne figurant pas du tout au répertoire.

Le moment est peut-être venu pour que le Conseil du Trésor précise mieux les renseignements que les institutions devraient décrire et la façon de changer leurs inscriptions. Il faut aussi qu'on examine de façon plus rigoureuse les renseignements que les institutions gouvernementales communiquent à *Info Source*.

Évaluations vers le haut

Dans des rapports annuels antérieurs, le Commissaire a exprimé des réserves quant à l'anonymat des évaluateurs qui faisaient des évaluations vers le haut dans certains ministères. Cette façon de procéder La donne aux fonctionnaires l'occasion d'évaluer le rendement de leurs supérieurs et de faire des commentaires à cet égard, souvent à titre anonyme.

Afin de déterminer à quel point ce procédé est répandu et comment il se déroule, la Direction de l'observation a fait un sondage auprès de 148 ministères et organismes assujettis à la *Loi sur la protection des renseignements personnels*. Au moment d'aller sous presse, le personnel de la Direction avait reçu 141 réponses, (dont 8 provenant d'un même ministère); 27 des ministères et organismes répondants ont dit avoir déjà recours à ce procédé ou prévoir s'en servir au cours des 12 prochains mois. Sur les 27, 24 ont promis de protéger l'anonymat des fonctionnaires évaluateurs et 18 emploient ou comptent employer des consultants du secteur privé pour l'analyse des résultats.

Bref, moins de vingt pourcent des organismes gouvernementaux ont retenu l'idée. Néanmoins, nous pouvons nous demander pourquoi l'administration fédérale devrait avoir recours à une procédure de relations du travail fondée comme celle-là sur le recours à des informateurs anonymes.

Gestion intégrée

La gestion intégrée assure à la fois au Commissariat à l'information et au Commissariat à la protection de la vie privée des services en matière de finances, de gestion du personnel, d'administration, d'informatique et de bibliothèque.

Ci-dessous les dépenses des commissariats pour la période allant du 1er avril 1991 au 31 mars 1992.*

	Information	Vie privée	Gestion intégrée	Total
Salaires	1 670 069	1 911 442	658 825	4 240 336
Contributions aux régimes d'avantages sociaux des employés	285 600	307 020	121 380	714 000
Transports et communications	75 621	59 500	124 875	259 996
Information	21 005	55 261	3 109	79 375
Services professionnels et spéciaux	209 028	190 237	81 059	480 324
Locations	4 391	3 276	11 945	19 612
Achats de services de réparation et d'entretien	6 688	6 358	7 199	20 245
Services publics, fournitures et approvisionnements	18 692	9 814	29 070	57 576
Acquisition de machines et d'équipement	109 474	44 361	12 959	166 794
Autres dépenses	2 970	1 873	250	5 093
TOTAL	2 403 538	2 589 142	1 050 671	6 043 351

* Les dépenses n'incluent pas les ajustements de fin d'année reflétés dans la section des comptes publics 1991-1992 traitant des commissariats.

Finances

Pour l'exercice financier 1991-1992, les ressources des commissariats ont totalisé 6 691 000 $ et 82 années-personnes, soit une augmentation de 367 000 $ et de quatre années-personnes par rapport à 1990-1991. Les dépenses au titre du personnel (4 954 336 $) ainsi que les services professionnels et spéciaux (480 324 $) représentent plus de 90 p. 100 des sommes globales. Les 608 691 $ qui restent ont servi à couvrir les autres frais.

Personnel

Dans le sillage de FP 2000, les services du personnel ont apporté plusieurs améliorations à leurs méthodes de gestion: recrutement d'une stagiaire en gestion, élaboration d'un programme de primes à l'initiative et d'un programme d'orientation pour les nouveaux employés et rationalisation de certaines procédures. De plus, les responsables du personnel ont effectué une vérification triennale de la classification, ont assuré le suivi de la vérification de 1987 sur les langues officielles et ont signé un protocole d'entente avec le Conseil du Trésor en matière de langues officielles.

Administration

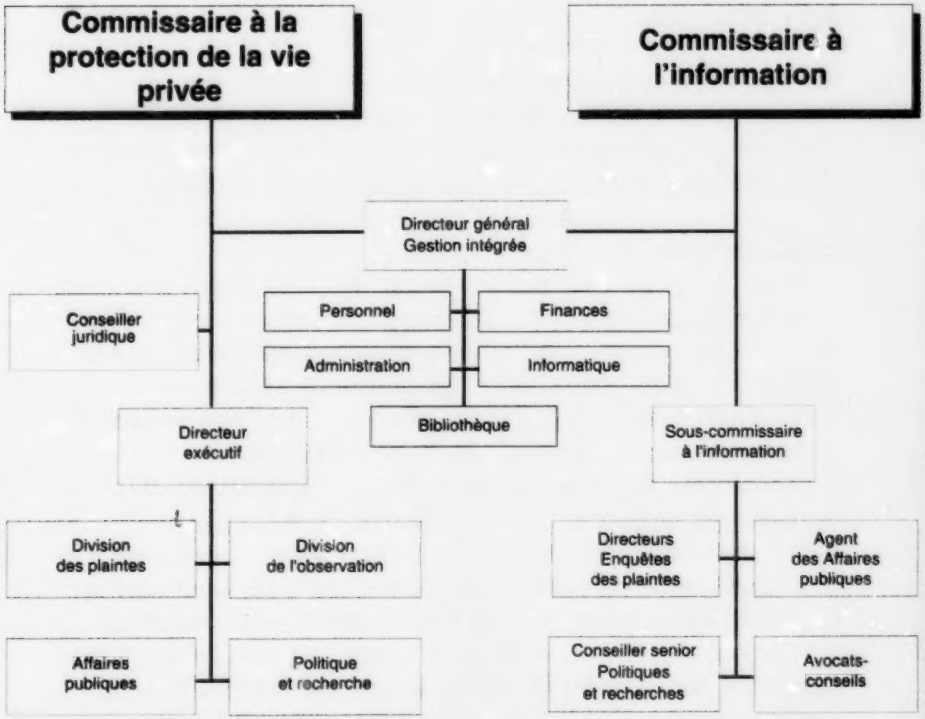
Les services d'administration ont continué d'avancer dans l'application du calendrier de conservation et d'élimination des documents et dans l'élaboration d'un répertoire informatisé des biens. De plus, le système téléphonique des commissariats a été évalué dans le but d'améliorer le service au public.

Informatique

Cette année, ce service a réalisé des études relativement à l'élaboration d'un nouveau système de gestion des cas, à la bureautique et à la mise en place d'un réseau informatique dans un contexte sécuritaire.

Bibliothèque

Les attributions de la bibliothèque concernent: les prêts entre bibliothèques; la documentation; les recherches manuelles et informatisées, ainsi que des dossiers thématiques de coupures de presse. La bibliothèque acquiert des ouvrages sur la liberté d'accès à l'information, le droit à la vie privée, la protection des données et la fonction d'ombudsman. Elle possède en outre une collection spéciale de rapports d'ombudsmans canadiens et étrangers ainsi que des rapports des ministères sur l'application des deux lois.

Au cours de l'année, la bibliothèque (qui est ouverte au public) a traité 1 298 demandes de prêts et a répondu à 1 084 questions à caractère documentaire.

Organigramme